University of Derby
Department of Computing & Mathematics

A project completed as part of the requirements for the BSc (Hons) Computer Networks and Security

Entitled

The network and security issues of BYOD (Bring Your Own Device) for Educational Institutions.

By
Kirk Lewis Kus
info@kus.org.uk
in the years 2015 – 2016
Abstract

This report investigates the network and security effects that come with BYOD (Bring Your Own Device) in general and then focuses on how it can affect an educational institution’s environment. The report then considers security solutions to tackle these issues with children’s wellbeing at the centre. Questionnaires regarding BYOD and wireless infrastructure were sent out to secondary schools and the findings and analysis have been documented in this report, together with a discussion about the problems and solutions. Finally the report suggests additional network and security recommendations for educational institutions which are planning on implementing a BYOD solution.
Acknowledgements

I like to thank my supervisor Kim Smith, who has given me feedback and suggestions on my dissertation. I would also like to thank Val Pickard, for helping with my dyslexia by checking my report for spelling and grammar mistakes.
Table of Contents

Abstract ........................................................................................................................................... 1

Acknowledgements ....................................................................................................................... 2

Table of Contents .......................................................................................................................... 3

1. Introduction ............................................................................................................................... 8
   1.1. Project Rationale ................................................................................................................ 8
   1.2. Project Aim and Objectives ............................................................................................. 9

2. Literature Review ...................................................................................................................... 10
   2.1. Introduction ....................................................................................................................... 10
   2.2. Background of BYOD ..................................................................................................... 10
   2.3. Benefits of BYOD ............................................................................................................. 11
       2.3.1. Organisational Benefits .......................................................................................... 11
       2.3.2. End user benefits ...................................................................................................... 12
   2.4. Security issues with BYOD ............................................................................................. 12
   2.5. Implementing BYOD ........................................................................................................ 15
       2.5.1. Network and costing ............................................................................................... 15
       2.5.2. Engage the community ............................................................................................ 16
       2.5.3. Develop a Team ....................................................................................................... 16
       2.5.4. Teachers ................................................................................................................... 16
       2.5.5. Pupils ....................................................................................................................... 16
       2.5.6. Head Teacher .......................................................................................................... 17
2.5.7. Parents, Community Members, and Board ...................................................... 17
2.5.8. Additional Support .......................................................................................... 17
2.5.9. Develop the Physical Infrastructure ............................................................... 17
2.5.10. Implementation example ............................................................................. 18
2.5.11. Develop the software infrastructure ............................................................ 19
2.5.12. Develop a portal .......................................................................................... 19
2.5.13. Develop an Acceptable Use Policy ............................................................... 19
2.5.14. Build a Curriculum ...................................................................................... 20
2.5.15. Consider Devices ......................................................................................... 20
2.5.16. Provide Ongoing Professional Development ................................................ 20

2.6. Threats and Attacks .......................................................................................... 20
2.6.1. Wireless attacks ............................................................................................ 20
2.6.2. DoS attack ..................................................................................................... 21
2.6.3. Cipher Attacks ............................................................................................... 21
2.6.4. Man-in-the-Middle ....................................................................................... 22
2.6.5. Eavesdropping .............................................................................................. 22
2.6.6. Mobile Applications ..................................................................................... 22
2.6.7. Malware ......................................................................................................... 23

2.7. Security for BYOD ............................................................................................ 23
2.7.1. Protection and security .................................................................................. 23
2.7.2. Incidents: Detecting and responding ............................................................. 25
2.7.3. Acceptable Use Policy .................................................................................. 26
9.2. Questionnaires from school 2 ................................................................. 69
9.3. Questionnaires from school 3 ................................................................. 72
9.4. Questionnaires from school ................................................................. 76
9.5. Questionnaires from school 5 ................................................................. 80
9.6. Questionnaires from school 6 ................................................................. 84
9.7. Questionnaires from school 7 ................................................................. 88
9.8. Questionnaires from school 8 ................................................................. 91
9.9. Policies document from school 3 ........................................................... 94
9.10. Policies document from school 4 ......................................................... 103
9.11. IT Policy for Staff - April 2015 from school 5 ...................................... 105
9.13. Social Media Policy from school 8 ....................................................... 118
1. Introduction

Technological advances in the 21st century have lead some educational organisations to use BYOD (Bring Your Own Device) for both employees and pupils. However security and network infrastructure can be a problem if BYOD is not set up correctly, therefore these security problems and solutions need investigating. There are fears that some that small-scale organisations may adopt BYOD too soon and without the correct network and security configuration placing themselves and their data at risk (Madzima, et al., 2014).

A reason for educational intuitions moving towards BYOD is that they will want increased productivity by their pupils and staff in order to improve their educational rating. BYOD allows users to access applications and data on their desktops using any mobile device, resulting in better productivity (AlHarthy & Shawkat, 2013).

Therefore with the growing demand for a BYOD solution within educational institutions, this report will be looking into the security of BYOD with a focus on schools and sixth form colleges catering for pupils from 11 years of age. The report will identify work that has already been done in the BYOD field generally and transfer these findings into a school environment. From the research, problems areas will be identified which will be analysed in order to suggest possible solutions.

1.1. Project Rationale

Information on BOYD found in journal articles, technical reports and websites usually focuses on the benefits, disadvantages, and statistics of BYOD in businesses and similar organisations. Many of these factors will apply to BYOD in educational institutions, however not all. More research is needed in order to specify the security implications of BYOD for educational organisations. With the research taking place purely in educational environments, additional recommendations for implementation can be made for schools that wish to apply BYOD solutions in the future.
1.2. **Project Aim and Objectives**

This project has many aims and objectives. First of all research will be done on the existing BYOD solutions and identify the current security problems and solutions. It will investigate further when these security issues are present in educational institutions and identify which security issues need addressing. It will gain recommended feedback from educational institutions on security implementations to help with the research and final recommendations. This report will also look at the network implementations of installing a BYOD system and identify installation processes for BYOD and how it can be modified to suit a more efficient process within educational institutions.

The project’s aim is to identify BYOD security issues in different environments and investigate the effects these issues potentially could have in an educational environment. Then further research will be undertaken to see if these effects have been taken into consideration by the organisation and how it has or would deal with them. Finally from all the research that is undertaken, my finding will be documented along with recommendations for educational institutions.
2. Literature Review

2.1. Introduction

This chapter will be looking at the different types of background research into Bring Your Own Device (BYOD) and different security effects that come with BYOD. This will help determine the areas of BYOD that need more research for tightening up the security aspects and for protecting data and information. Due to the nature of the system, a great deal of research has already been done in businesses and organisations concerning BYOD technology. This research will be examined and analysed in order to suggest procedures that will help identify problems and solutions that can occur in educational institutions.

2.2. Background of BYOD

Bring Your Own Device (BYOD) is a policy that allows or encourages employees and pupils to use their own mobile devices on the original network (Evans, 2015). However does comes with BYOD security concerns that need to be addressed, this will be discussed later in this paper.

The first instance of the use of BYOD can be found when individuals brought memory storage devices into educational institutions to transfer data. Security software can and has been implemented in educational institutions to disable USB ports. This is to combat security threats and possible downtimes. However educational institutions are pushed towards using BYOD due to its massive benefits and for the school to become more competitive. The benefits of BYOD will be discussed later in this paper. Educational institutions are placed into a relevant league table and their position in the table is based on their performance (UK Government: Department for Education, 2016). This creates competition between each institution in the area and nationally. Parents will want to place their children in the higher ranked school to increase their children’s chances of a better education. Therefore if BYOD shows that it improves performance of both staff and pupils then more schools will be encouraged to implement BYOD in their organisation.

When looking at the security of BYOD they are three aspects that need to be taken into consideration: people – who is going to use it and its accessibility; policy – the organisation’s policy that users have to adhere to; technology – what technology will be used and allowed
onto the network. As the devices connecting to the network on BYOD technology are privately owned this presents a new challenge for the organisation’s IT infrastructure as they will have to evaluate how safe their data, assets and information systems are from being lost, stolen or misused.

In an educational environment it makes logical sense to split the users of BYOD into categories as each one may not need the same access to the network. The three groups are as follows: pupils, staff and guests. Pupil’s access will depend on the educational institution’s requirements. For example do the pupils need access to the network (personal home drive or shared area) or just the internet connection? Staff may need to access certain software or have access to the intranet to do class registers or to write reports etc. The guest’s network is usually for guest speakers and generally they will only need access to the internet.

The future of BYOD looks to increase especially in educational environments as research shows the number of mobile devices among children is increasing year upon year. A survey (Rideout, et al., 2010) showed that in 2004 children between the ages of 8 – 18 years owned the following: iPod/MP3player 18%, mobile phones 39%, laptops 12%, and in 2009 the figures were iPod/MP3player 76%, mobile phones 66%, and laptops 29%. This shows that over time there will be greater demand for educational institutions to adapt and use BYOD to become more competitive as more and more pupils bring their own personal devices to schools.

2.3. **Benefits of BYOD**

This section will observe the benefits of BYOD. This will help report why educational institutions are moving to BYOD.

2.3.1. **Organisational Benefits**

This section will look at the benefits that BYOD brings to organisations. This will help show why organisations are moving towards BYOD. BYOD has many advantages for any organisation to increase users’ productivity and decrease the company’s costs of computing assets, licensing, software, insurance and procurement (Wang, et al., 2014). In educational institutions assets can get damaged very easily by careless actions by students however people are more likely to look after their own devices (Alliance Solutions, 2014). This is down to two factors, firstly the device is usually purchased by the user and secondly it contains personal information as well as information from the organisation (Gajar, et al., 2014). The benefit for
educational intuitions to implement BYOD is that software and tools are available on BYOD networks for both students and staff to use. For example, the Kahn Academy and the Harvard/MIT edX (www.edxonline.org) are some of the organizations that provide alternative, low-cost, yet high-quality online educational opportunities for BYOD consumers (Miller, et al., 2012).

2.3.2. End user benefits

This section will look at the benefit that BYOD brings to end users. Enabling BYOD is pointless unless you have people using it. Therefore the benefits to end users will be identified in this section to show the reasons why people will use BYOD.

The benefit to pupils within an educational institution using their own devices is that they are not limited to the software that is available on the school’s network as they are able to download and install their own software onto their machines. Teachers and pupils are often more familiar with their own machines and are able to use them more efficiently (Bennetto, 2013). Both students and staff using BYOD are able to do their work on their mobile device such as laptops, which allows them to take it home and carry on with their work without saving it onto an external storage device such as memory sticks, which can easily be lost.

In most educational organisations the number of computing devices in an institution is not enough for everyone to use at once, however people bringing their own devices to use reduces the burden on the school’s resources. Another benefit of students using their own devices is that, when they are working on their own device they tend to have more satisfaction, be more productive and have greater work mobility, as they can freely move around and carry on with their work (Capgemini Consulting, 2013).

2.4. Security issues with BYOD

BYOD does have a darker side. If BYOD is not fully implemented, regulated and understood, it can threaten IT security and put the organisation’s sensitive information at risk. This section will look at the security issues associated with BYOD networks and why it is important to fix these issues.

The challenges for BYOD in an educational environment are personal data and child welfare. An example of a possible security threat is a teacher could store personal information from the school’s data such as a child’s confidential information on her own laptop, the laptop could
then be lost or stolen or the information transmitted unintentionally or even intentionally. These things have to be addressed for a child’s safety and The Data Protection Act 1998. This is backed up by a study by Webroot in 2014. The survey (webroot, 2014) shows that 98% of employers have some kind of security policy for mobile data accessing the corporation’s data. 21% of the people sampled stated that their organisation allows employees to access the data with no security at all. The report also showed that only 19% of people installed a full security app and that 64% of employees admitted only using the basic security features that the device was preinstalled with. If the same statistics apply to educational institutions, this needs to be addressed by having policies setting out the best practices and the do’s and don’t for the user when using the IT infrastructure in a workplace. The policies are there to prevent IT misuse and ensure data is secure and is not leaked. However a worrying factor is that organisations with BYOD systems have little to no technologies and/or policies in place (Zahadat, et al., 2014). This has to be addressed and especially in educational organisation where children’s safeguarding could be at risk.

To prevent data from being leaked or being stolen by different attacks, the people in an organisation should be taught the basic security and wireless security best practices. However a report shows that as many as 80% of companies surveyed lack this critical component, and do not teach employees how to prevent inadvertently sharing or exposing sensitive data and information (Greengard, 2014).

A report by Trend Micro (Trend Micro, 2013) shows some interesting figures to do with IT security. The report show that 27% of the people who participated in a survey have had up to 3 work devices lost or stolen. This is a high number of work devices that have gone missing, the data on these digital devices could be confidential, therefore extra security measures such as BIOS passwords and BitLocker could be required. The report also states that 31% of the people surveyed regularly use WiFi hotspots, and 56% of these never or rarely check the security level before using a hotspot. This can be addressed by training employees to help them understand the best practices of security and wireless security when using a work or personal device that contains sensitive information outside of the workplace. The report showed that 63% of people in the survey use the same passwords or similar variations for all their electric logins. This can be addressed in security training sessions and the IT department can enforce IT policies that makes users change their password after a set amount of time (for example every 60 days). However it does not seem that staff are getting any education from their company or employer as the report from (Trend Micro, 2013) identifies that IT
department should be concerned about the education of staff within the organisation. 56% of people who took part in the survey said they did not know what to do to protect the data on their devices if they are lost or stolen. Only 10% said they would contact the IT department. On top of training, it is advisable for the IT department to offer a service and/or educate staff how to erase data from their personal devices if they are getting rid of them or selling them, as it can contain personal information. Using the ordinary way of deleting information from a hard drive only marks the data as erasable and can be easily restored using recovery software (Gizmodo, 2010). Software is available to properly erase all the data from a hard drive by making the data either ones or zeros (James, 2015). When it comes to sensitive data the organisation and the staff should fully understand how to destroy it, or a service should be offered by the organisation. The ICO (Information Commissioner’s Office) which is an independent authority in the UK set up to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals, states the following:

“It is good practice to make it clear to people what will happen to their information when they close their account – i.e. if it will be deleted irretrievably or simply deactivated or archived. Remember that if you do archive personal data, the rules of data protection, including subject access rights, still apply to it. If you offer users the option to delete personally identifiable information uploaded by them, the deletion must be real i.e. the content should not be recoverable in any way, for example, by accessing a URL from that site. It is bad practice to give a user the impression that a deletion is absolute, when in fact it is not.” (ICO, 2015)

They are two main laws that have to be taken into account in the UK, they are the DPA (Data Protection Act 1998) and Computer Misuse Act 1990. Breaking the Data Protection law can result in a fine up to the sum of £500,000 (ICO, 2013) and breaking the Computer Misuse Act 1990 can result in up to 5 year’s imprisonment and a fine that is not exceeding level 5 on the standard scale which is a fine up to £5,000 (The UK Government, 1990). The survey indicated that people take better care of their own personal devices as only 11% of people lost their personal device or had it stolen compared to 27%, who lost up to 3 work devices. This shows BYOD can bring extra security benefits to an organisation as less people are likely to lose their personal device than a work device. In addition the survey showed that 44% of people surveyed were more worried about losing personal information such as photos and banking information than sensitive corporate information. This indicates that a person using
personal devices on a BYOD network will look after them better than a device given by the organisation, and less likely to breach any security policies.

2.5. **Implementing BYOD**

The implementation of BYOD requires a lot of thought and planning in order to successfully work efficiently. The K-12 Blueprint report (K-12 Blueprint, 2014), has very good documentation that outlines the steps that need to be undertaken when implementing BYOD in an organisation. The plan is generic and not specific for educational institutions. The steps are as follows:

2.5.1. **Network and costing**

A question that will need to be asked is whether the network can handle more traffic on the existing network. Having BYOD will in time increase the number of devices on the network therefore resulting in more networking overheads and needing additional bandwidth. The report (Loucks, et al., 2013) shows the costs of implementing BYOD and as more devices connect to the BYOD, upgrading the networking infrastructure may be needed to handle the extra workload. The costs of maintaining and upgrading the network due to BYOD all depends on many different variables which change dependent on different circumstances. The costs of hardware, software and licencing BYOD with the cost of potential upgrades have to be considered. However the report (Loucks, et al., 2013) states that in the long term the cost of BYOD will be reduced in other areas of the computing budget making it a worthwhile investment. The savings come from reducing the licencing needed as staff can use their own software on their own machines. The IT budget for machines can be reduced as more staff bring their own machines to the organisation (BYOD.US, 2013).

Other additional costs from the report (Loucks, et al., 2013), show that with a typical upgrading cost of implementing a comprehensive BYOD system, 37% of the total cost will come from upgrading the software, for example collaboration tool licenses. 26% of the total upgrading cost comes from policy and security, this includes the policy management, implementing/updating the AUP and MDM (Mobile Device Management). 19% of the total upgrading cost comes from network and operations, this includes the WiFi access points, network management and maintenance. 14% of the total upgrading cost comes from Telecoms, this includes the upgrade or changes to the WAN system, for example increasing broadband bandwidth and capacity. The rest, 4% of the total upgrading cost comes from
support and training, this includes the training for using the BYOD system and the support from the help-desk.

2.5.2. **Engage the community**

The report suggests the first step should be to engage the community. In educational institutions this would include staff, students, parents and the institution’s board members. Consulting with these people will help build a picture what people expect from BYOD. Also by consulting parents and pupils it is then possible to gather information on how many people within the organisation that have mobile devices that they are able to use within the school.

2.5.3. **Develop a Team**

The report suggests creating a team for implementing BYOD. The core team is advised to consist of the head of eLearning and other technical specialists who support the institutions its technological initiatives. The report also adds that additional responsibilities should be included such as detailed planning, exploring new technologies, planning professional development, and troubleshooting.

2.5.4. **Teachers**

Teachers who want to use BYOD for eLearning technologies should also be considered to help with the planning so that the locations and amount of wireless AP can be taken into consideration. Teachers may also want to trial different types of eLearning technologies and platforms. Research into different types of eLearning software can be done by the teachers and IT staff.

2.5.5. **Pupils**

The report recommends that the educational institution should consider input from students. This can be done by all students or by consolidating some keen students into a focus group. The pupil’s objectives in the group would be to learn new eLearning, assist teachers with technology needs and help choose and research which eLearning technologies would be best for the organisation. Also a good incentive is advisable to encourage students to participate in the project.
2.5.6. **Head Teacher**

With the head teacher attending the meetings he/she will be able to offer their thoughts and views in the meetings and broaden the extent of conversations and gain further insights. The head teacher should also be notified of any changes that the school is adopting.

2.5.7. **Parents, Community Members, and Board**

Parents can offer their support on a voluntary basis on the project-specific teams, suggested by the report. A BYOD technology scheme directly affects parents, therefore their input should be considered as part of the plan for BYOD and eLearning. With many schools being academies, community funding can be an option from the board members and the backers of the academy.

2.5.8. **Additional Support**

The report also suggests the makeup of the additional support team, if required. The role of additional support is to attend eLearning team meetings or lend support on project-specific teams. It recommends that the team should consist of: headmaster, project manager of the technology team, multi-media designer and district directors.

2.5.9. **Develop the Physical Infrastructure**

The third step on the report (K-12 Blueprint, 2014), is the development of the physical BYOD infrastructure. The key points to take into consideration from the report are the following:

The network bandwidth and the wireless AP bandwidths have to be taken into consideration, for example will an AP and the network be able to handle a full class using the system. The location of the AP should be considered, the times when pupils need access to the network will have to be taken into consideration as will what kind of network activity students will be using, as multimedia applications will need a high bandwidth.

The report suggests contacting specialists to help setup the BYOD. It also informs that BYOD brings security concerns, which need to be addressed to comply with the Data Protection Act 1998.

A protective wireless infrastructure has to be implemented into the BYOD network to ensure only authenticated users can log onto the network. Built-in authentication mechanisms enable
monitoring of internet usage. A protective wireless infrastructure for the BYOD project provides a separate section for students and pupils on the network to prevent data security conflicts and to protect student information.

Also it is important to have the capability for growth for the BYOD technology and for the network to handle more bandwidth because of the effects of people bringing more portable devices into the organisation.

2.5.10. Implementation example

In the report (K-12 Blueprint, 2014) there is an example of BYOD in a school in America called Oak Hills. Here are the technical elements they have implemented:

Wireless Infrastructure:

*Cisco Dual-Radio wireless access points*

Strategically positioned to minimize RF interference between each other

Provides approximately 95% building coverage for wireless G standard devices

Network:

Network configuration consists of multiple SSID’s (networks).

Security maintained with a separated network configuration that includes a staff network, student network, and guest network

Staff and Student network is secured via WEP, and is available to any employee or student utilizing district owned equipment

Guest network is an open SSID, allowing any student- or staff-owned equipment to access the internet

*VM Ware*

8 Cisco UCS Blade servers arranged in two 4-blade chassis. Each Blade consists of:

(2) 6 core processors for a total of 12 cores per blade

192GB of RAM
This is a total cluster wide of 96 CPU cores, and 2.3 Terabytes of RAM

Cisco UCS Fiber interconnect

Netapp Fiber Channel SAN storage, with 7 TB of storage on SAS 15k RPM drives

Running VMware ESX, and VMware View5

(K-12 Blueprint, 2014)

2.5.11. Develop the software infrastructure

With BYOD the organisation will have multiple devices connecting to the network and for eLearning purposes it is important to see what software is available for different types of platforms. Web based software for example can be accessed by the majority of devices as long as they have a typical version of a web browser. This allows pupils to do their work on their own device, devices from school and even at home if the web based software is available for external use.

2.5.12. Develop a portal

Once the tools and resources have been agreed for students and staff to access, the report advises the development of a portal for students to go to. This is also known as a landing page and is the first page people see when accessing the BYOD network. This then has the links to useful websites, software and bulletins. The landing page should be able to be viewable from multiple devices such as laptops and mobile phones.

2.5.13. Develop an Acceptable Use Policy

An Acceptable Use Policy (AUP) should be adapted and established with the BYOD system, this will say when and what devices can use the BYOD and in what manner. The educational institution should already have an AUP therefore it may just need tweaking for BYOD. At the beginning of each school year the students and staff should read and sign the AUP agreement which can be done via paper or electronically. Anyone breaking the policy should be subject to disciplinary action; this will act as a very good deterrent and will benefit the security of the system from anyone breaking the Computer Misuse Act 1990. Also the IT department should have the capability to monitor the network for any wrongdoings.
2.5.14. **Build a Curriculum**

This depends on the scope of use of BYOD for the school. Teachers may want to use BYOD for students to access resources and be able to do work on their mobile devices. Mock exams and tests can also be uploaded to schools network for pupils to complete which can also give feedback/results straight away.

2.5.15. **Consider Devices**

The report suggests not to totally rely on pupils bringing their own portable devices as some may not have them, the specifications are not good enough or they may not be able to afford them. The school could also offer a suggested specification for students if they want to buy a new device which will efficiently run the different software that is available on the BYOD network. The device’s battery life is of concern, therefore a device with a good battery life will be advisable however the number and positions of plug sockets for recharging will also will need to be taken into consideration.

2.5.16. **Provide Ongoing Professional Development**

Once BYOD has been implemented and installed in the educational institutions then ongoing support and help will be needed if BYOD is to be a success. This includes monitoring the effects and uses of BYOD as well as offering training for staff and pupils. In the future, the number of devices and their usage on the BYOD network will increase therefore the network activity will have to be monitored for possible future expansion.

2.6. **Threats and Attacks**

This section will be looking at the different types of attacks that a BYOD network environment can suffer, including wireless attacks, malware and other attacks that are a threat to BYOD.

2.6.1. **Wireless attacks**

As most devices in a BYOD network are connected wirelessly, the majority of the attacks will be focusing on attack methods on the wireless system.
2.6.2. DoS attack

Denial of Service (DoS) is an attack that is preformed to halt or interfere with the service, making the service unusable or affecting the legitimate function of the system (Basta, et al., 2013). In a wireless environment there are different types of DoS attacks that can be performed. The main wireless DoS attacks are the following:

Jamming – This is where an attacker sends radio frequencies on the same radio spectrum as the organisation’s network (2.4GHz or 5GHz) to create interference (Pelechrinis, et al., 2011).

Authentication / Association Flooding – this is where an attacker will ‘flood’ an AP (Access Point) with authentication requests and association frames. The attacker can change its MAC address in order to impersonate many different clients (Singh & Sharma, 2011).

De-authentication Flooding – this is where an attacker sends de-authentication packets to clients that are connected to an AP. This can easily be actioned by an attacker as the frames sent are in plain text (K’Ondiwa & Ochola, 2013).

EAP (Extensible Authentication Protocol) – This is where the attack is on a protected wireless network and floods the network with EAP authentication requests (Alruban & Everitt, 2011).

As mentioned in the reports that identify the different DoS attacks, they can be detected and/or prevented with an adequate wireless IDS (Intrusion defence systems) and IPS (intrusion prevention systems) (Alruban & Everitt, 2011) (K’Ondiwa & Ochola, 2013) (Singh & Sharma, 2011) (Pelechrinis, et al., 2011).

2.6.3. Cipher Attacks

Some cipher attacks include breaking the WEP (Wiired Equivalent Protection) encryption key. WEP is however a very weak and old security method that can easily be cracked (Kipper, 2007). The more secure option for wireless protection on a network is using WPA (Wi-Fi Protected Access) or WPA2. However WPA still has some weak points. WPA is prone to a dictionary attack. This vulnerability can be made easier for the attacker if the passphrase is left as default, or the password to gain access to the network is simple and/or short (Thornton, Rogers, & Hurley, 2006). Using WPA/TKIP presents vulnerability where it is possible for attackers to decrypt the data (Dunkerley & Samuelle, 2014). Another attack can be performed on the LEAP (Lightweight Extensible Authentication Protocol), as LEAP credentials are not
strongly protected, this leaves it open for attackers to perform dictionary attacks (Butler, et al., 2007).

### 2.6.4. Man-in-the-Middle

A MITM (Man-in-the-Middle) attack is where an attacker attempts to insert themselves in-between the communication system of two devices. In this case the attacker will try and lodge between a client and the Access Point and secretly relay information between the two devices. The attacker can also achieve this by acting as an AP on the network, and then relaying information onto a legitimate AP when a device connects to his rogue AP, this method is called Evil Twin (Low, 2005). Software is available to prevent these attacks from happening and Cisco has solutions that prevent these attacks, for example identifying additional AP on a network that could be a rogue AP (Cisco, 2006).

### 2.6.5. Eavesdropping

Eavesdropping is a method of attack, where the attacker listens to the RF (Radio Frequency) to gather information from what is being sent from two devices. This technique is easier for the attacker to perform if the wireless network is unprotected therefore the data being sent is not encrypted. Ensuring the data is encrypted between the two devices and it is not an open security network will prevent attackers performing an eavesdropping attack (Coleman, et al., 2011).

### 2.6.6. Mobile Applications

With mobile devices connecting to the organisation’s network, issues such as Zombie Application can cause a security threat to the organisation. Zombie Applications are applications that are no longer available on the respected store (e.g. Apple App Store or Google Play Store) and no longer supported. These apps may have been removed from the store due to flaws with security such as compromising user privacy or enabling malware delivery. Another reason is that the applications are no longer being updated and therefore carry security vulnerabilities (Gamer, 2015). A report from Appthority investigated the number of Zombie Applications on both Apple and Android with 3 million devices, the report showed that 5.2% of Apple applications on the device were Zombie applications and 3.9% on Android were Zombie applications (Appthority, 2015).
2.6.7. **Malware**

Malware is any software that is used to damage or change the computing operations, gather private or sensitive information or gain access to the network. Some examples of Malware include computer viruses, Trojans, Worms and Spyware (Aycock, 2006). Personal devices being connected to the network will increase the threats of Malware being on the network. This is because the security settings and antiviru software on the device may not be configured correctly or even installed.

2.7. **Security for BYOD**

This section will talk about the security of BYOD to defend and prevent against attacks. The biggest concern regarding the implementation of a BYOD system is the security (EY Foundation, 2013). The (EY Foundation, 2013) report shows that the greatest concerns when implementing BYOD are: Mobile device security 65%, data breach security 59%, mobile data security 55% and mobile application security 50%. These outweigh the other concerns such as costing.

2.7.1. **Protection and security**

Most digital devices support two way authentication mechanisms such as access cards, token codes or biometrics which should be considered for the extra security for staff accessing their devices on the network or for reading confidential data. However this will add another costing to the BYOD framework. The decision of whether to use one way or two way authentication between the devices and the node wirelessly has to be taken into consideration. One of the most important aspects of wireless security is the key standard that is used. Wireless protection standards have evolved in time to deal with the increase in security issues. The best wireless standard to use today is WPA2 rather than WPA or WEP (Stewart, 2011). For wireless connections outside the workplace it is recommended to choose a connectivity that has wireless encryption. Another option is to implement VPN (Virtual Private Network) on teaching machines this then has the advantage of security solutions that utilise an “always-on” VPN solution that runs through the corporate network. The VPN solution protects the confidentiality and integrity of communications between the end users machine and the network (Merkow, 1999).

Another way of protecting the network and devices in a BYOD network is to use MDM (mobile device management). MDM is a piece of software that manages, monitors and
supports mobile devices on the network. MDM functions usually include ‘over-the-air’
distribution of applications, and data and configuration settings for all types of mobile devices
(Intelligence, 2013). The benefit of MDM is that it allows the organisation to control and
protect the data and configuration settings for all mobile devices on the network, therefore
reducing support costs and risks to the organisation. The main purpose of MDM is to optimise
the functionality and security of the mobile devices on the network and reducing the costs and
downtime (Intelligence, 2013). The EY report on BYOD (EY Foundation, 2013) also advises
to consider investing in MDM to increase mobile device security on a BYOD, to impose
policies and monitor device activities.

Setting a baseline in the BYOD network can reduce the security threats and attacks to the
organisation’s system. A baseline is a policy that conducts a set of objectives which must be
met to be able to rightfully use the device on the network (CERN, 2010). The purpose of the
security baseline is to ensure that devices have an adequate and appropriate level of security.

An important element for security backed up by the research from above in the ‘Security
issues with BYOD’ section, was the training aspect of employees using IT in an organisation,
as IT knowledge is lacking and training is often not proved therefore must be addressed.
Training and educating people of the security effects inside and outside of work should be
addressed especially to those who will be dealing with personal and confidential data. A
report on the BYOD security engineering framework (Zahadat, et al., Olson, 2014) outlines
training procedure that should be conducted for an organisation with BYOD. It states that
training should be provided at the outset and users should go through the training before using
the BYOD network. The training should be repeated annually and should include the aspects
of BYOD program which includes users responsibilities, regulations protecting them, their
data and the security requirements. Also as the above in the ‘Security issues with BYOD’
section indicates, an issue is employees reporting lost or stolen devices to the IT department,
therefore the training programme should also teach employees the protocols to action when
this happens.

Encrypting data transmissions is essential for BYOD security. Encrypted VPN connections
using IPSec provide confidentiality and integrity (Frankel, et al., 2005). However this method
only keeps the data transmission encrypted, once stored on a machine it may no longer be
encrypted. To rectify this issue, enabling or changing security settings on the mobile device
for encrypted stored data must be embedded. Some mobile devices such as the Apple iPhone
3GS or newer has a full hardware encryption utility using AES-256 and this level of security cannot be disabled (Zahadat, et al., 2014).

2.7.2. Incidents: Detecting and responding

When an incident happens on the network, vulnerabilities can be exploited or if malicious software is installed on the network and is not either detected or dealt with, then an attacker can use this to gain a foothold onto the network. A foothold could enable attackers to gain access to data that otherwise should be restricted (Rockwell Automation, 2009). The ‘Security issues with BYOD’ (Zahadat, et al., 2014) states that in a corporation’s network the SIEM (security Incident and Event Management) solution, IDS/IPS (Intrusion Detection/Prevention Systems), and/or Next-Generation Firewalls should be configured correctly on the network. This will help detect malicious activity, rogue devices or equipment trying to gain access onto the network. Most wireless AP (Access Points) such as Cisco’s 1000 series automatically detect and collect information on rogue AP, detected by its managed access points and then issues a warning to the IT department, which includes the location of the rogue AP (Cisco, 2006).

Even with all the safeguarding in place it has to be presumed that devices will go missing in the future therefore an adequate plan is needed to deal with a scenario where a device does goes missing. In the BYOD security engineering report (Zahadat, et al., 2014) it rightfully states that included in best practices procedures there should be a system in place whereby staff are trained for the scenario of a device going missing or stolen. The protocol for a device that has gone missing or stolen is to let the IT department know as well as the police etc. The IT department then can disable access to the organisation’s data from that machine.

When it comes to data, it can be lost, leaked or stolen. To prevent and detect this, systems such as Data Lost Detection or Prevention (DLP) solutions can be used. DLP is designed to monitor, detect and block sensitive data from potential data breaches and data ex-filtration transmission. The DLP can be sited at a strategic network location to allow the monitoring of all BYOD data transmission (Fortinet, 2011). While the idea of having faith in employees to keep the data secure, would be ideal, a survey from Symantec found that more than half of employees emailed work to their personal account, 41% downloaded information to their mobile device and 37% used cloud storage systems such as Dropbox or Google Docs to store their company’s data; all without permission (Symantec, 2013).
2.7.3. **Acceptable Use Policy**

AUP (Acceptable Use Policy) is the set of rules that users have to adhere to. The policies are in place to ensure users are using the system correctly in order to protect the security of the network. AUP are used to prevent users introducing viruses or any other attacks on the network. The AUP policy is needed at the beginning of any computer organisational network. The AUP should be enforced on all users on the network and the policies should be kept up-to-date with the changes to the network (Shinder, 2006). However as mentioned above a worrying factor is that organisations with BYOD systems have little to no technologies and/or policies in place (Zahadat, et al., 2014).

2.8. **Conclusions**

Much research has already been carried out into BYOD system in the business field however not in the educational field. The figures from some of the findings above would be quite distressing if the same responses are found in the educational field, as student’s personal and confidential information could be at risk. Some of the issues and security threats that come with BYOD can be resolved in many ways; however IT professionals could provide practical and expert input into the formulation of the recommendations.

BYOD does come with a lot of benefits as discussed above, however it does also come with increased security threats that need to be addressed by the organisation. Some of these threats can easily be dealt with if security measures are implemented correctly. Identifying the biggest security issues in educational bodies will help determine the recommendations of this report.

2.8.1. **Key Issues**

Some key issues that I have found are: 19% installing a full security app and that 64% of employees admitted only using the basic security features that device were preinstalled with (webroot, 2014). This can be addressed by training or offering information on how to keep your mobile device more secure by installing Anti-Viruses and keeping the operating system up-to-date.
Many organisations with BYOD technologies have little to no technologies and/or policies in place (Zahadat, et al., 2014). This can be addressed if the same issue is found within educational institutions. Enforcement and awareness of policies should be understood by all users using the system. Information on different policies can also help with the final recommendation.

11% of people lost their personal device or it was stolen compared to the 27% of the people participated in a survey have had up to 3 work devices lost or stolen. The report also states that 31% of the people surveyed regularly use WiFi hotspots, and 56% never or rarely check the security level before using a hotspot (Trend Micro, 2013). This can be addressed by educating safe that have access to pupils: details, personal data and confidential information.

2.8.2. Refined Research Questions

The aim of the project is to look at the security effects of BYOD in educational institutions. The main focus will be looking at the BYOD in schools to ensure the safe guarding of children’s personal and confidential is secure. The research and finding is to help produce a recommendation guide that can be used to increase security and help the information getting into the wrong hands.
3. Research Methodology

3.1. Introduction

The aim of this project is to identify security threats and security solutions of BYOD specifically in educational institutions. Once these have been identified then a recommendation will be produced at the end of this report. The research objective is to gather information on attacks, concerns and security implementations that have been undertaken in the educational field.

3.2. Research Strategy

This section will look at different research strategies that can be used to gather information, and their effectiveness in reaching the research objective. The following research strategies could be used:

**Interview** – An interview can be used to ask individuals specific questions to gather information and data. The interviews can be one-to-one or in groups, which will widen the dynamic of the discussion and allow interaction. A one-to-one interview can allow an individual to open up as it is more private. This is best used to ask certain individuals who are experts in their area to gather information or feedback. However in this case, the aim is to identify that there are common security issues that need addressing therefore a research strategy that has a large sample size will be better suited.

**Questionnaire** – A questionnaire is a practical way of gathering information en masse. A questionnaire can be created then emailed, handed or posted out to many different people or organisations. The answers can be compared easily as most questionnaires mainly consist of binary answers and can be analysed more scientifically. The negative effect of questionnaires is that they can limit the outcome of the answers, as most answers are given in binary (yes or no). There is no way of telling whether the respondent is being truthful. People’s interpretation of a question and answer may be different, for example someone’s ‘excellent’ maybe someone else’s ‘good’. In this research to identify common security issues, concerns and solutions with BYOD a questionnaire will be sent out en masse to reach a greater target audience.
Simulation – A simulation can be run on either a computer or a network of computers to mimic and reproduce the behaviours of a system. In this case a simulation could be used to mimic a BYOD environment and then test the outcomes of different attacks and security methods. However a lot of this research on security solutions has already been done and discussed in the literature review. Also this will provide little additional information on the objective this paper is trying to achieve. The simulation would also be better using hardware to imitate the outcome however this can be expensive.

Literature review – The literature review and future research can be used to compare previous results and outcomes to identify certain aspects. In this case security issues and concerns can be identified by examining previous research and results. Gathering different data and solutions from a range of different sources can help produce a final recommendation that covers the different research methods that have already been done and enable the best one for recommendation to be selected.

3.3. Data Generation Methods

The process of gathering information for this research will consist of two methods, firstly, a questionnaire to gather information to justify the purpose of this research. Secondly the research will also explore the dangers that affect BYOD systems covering both theoretical and real-life attacks that have happened in educational institution environments. The questionnaire will also help explore solutions for these problems and help find solutions that school networks have already undertaken to help tackle these security issues.

There will be two questionnaires to increase the target audience, which in turn will hopefully increase the number of responses. The first questionnaire is for educational institutions that have already had a BYOD system installed in their network. This will ask about the BYOD system and security threats that have happened to the network as well as security solutions on the system. The majority of these answers can be answered via tick boxes which enable the data to be categorised easily. The second questionnaire is to be filled by educational institutions that have not got BYOD systems installed. However it will look at the threats they are concerned about and attacks that they have experienced on the network as well as security mechanisms they already have in place to protect their system. Most of the questions from the two questionnaires and binary outcomes overlap therefore the data can be gathered together at ease.
The questionnaires will be sent out to schools requesting for the IT department to fill them out and sent back to me. The schools chosen will be selected randomly based on geographical location in the UK, however the schools that are being targeted are secondary schools and sixth forms in the UK.

To gather information to identify security issues and threats a questionnaire will be sent via email for IT technicians with educational institutions to fill out. The questionnaire will collect quantitative data on the range of security threats and issues that BYOD comes with. The questionnaire will be sent en masse to secondary schools and sixth forms across the UK.

3.4. **Data Analysis**

As mentioned above both questionnaires are designed to have questions and answers that overlap therefore they both can be used when gathering information. The questionnaires are also designed to give both binary and non-binary answers. The binary answers will be easier to examine, categorised and compared with previous work that has been carried out in this area. Non-binary questions that require writing out an answer will then need to be examined and then this information can be used in the discussion to help determine security solutions in the recommendation.

The questionnaire objective is to be able to analyse security issues that exist. These questions are mainly binary questions to identify security vulnerabilities or past attacks that the institution has faced before. Also questions are available for the IT Department which will be filling out the questionnaire to provide details of security measures or to advice on other security measures that they have in place. This will help in the discussion section when looking at security mechanisms in order to keep BYOD technology secure in educational institutions.

3.5. **Sampling**

The questionnaire will be sent out to over 1,000 different secondary schools and sixth forms across the UK, however the expectation of returns will be low which is normal with any type of questionnaire that gets sent out to businesses and organisations. All data received will be analysed and used in the analysis section of the report to help identify problems. The results and analysis of the results will be discussed below.
3.6. **Ethics**

All data gathered will be kept confidential and numbers will be used rather than names to identify the institution. This will avoid highlighting which schools could have which potential threats. However all schools that take part in the questionnaire will be sent out the final recommendation for schools to secure BYOD technologies.

3.7. **Limitations**

The limitation with the research is dependent on the number of responses that are received from the questionnaire. Some of the questions may not be known by the IT technicians that work in the organisation. Also the non-binary questions will need to be analysed and examined.

The issues with using questionnaires as mentioned above is that the truth of the answers cannot be guaranteed and relies on the person filling out the questionnaire to be honest. Another limitation with the questionnaire is that in order to get a good response the questions cannot be too many, too long or too complex or it will put off the person involved with the questionnaire.

The issue with confidentiality can be a concern for the people filling out the survey. If the questions being asked are confidential or the answers given can be used against the organisation then the person filling out the data will be reluctant to fill out this data. Therefore the questions being asked have to be valid reasonable questions that will get a response.

3.8. **Conclusions**

The methods of gathering information will be conducted in two ways, questionnaire and research. The questionnaire will be to gather information about security issues and vulnerabilities within educational organisations. The questionnaire will also help find possible solutions for these concerns which can be discussed and researched in the later sections of this report. The questions that are going to be asked will also not be too lengthy or complex however the information needed will help with the further research in this project. To encourage people to fill out the questionnaire the ones who participate will be sent the recommendation once it has been completed in this report.
4. Findings and Analysis

4.1. Introduction

This section will look at the results of the questionnaire and relate this with the findings from the research in the literature review. The key findings from the questionnaire will be posted below and discussed as well as any issues that have occurred. This section will also include how the study could be improved for future research in this area.

4.2. Analysis

This section will look at the different data and feedback given by the different educational institutions.

4.2.1. Key findings

The questionnaires found both positive security implementations and security threats. The positive security answers show that the schools have addressed security issues in order to combat and prevent attacks. Every questionnaire received back uses the highest wireless security encryption standard of WPA2. This WPA2 is the highest wireless encryption method that can be used on a wireless network and is more secure than WPA and WEP.

Only one of the questionnaires received back experienced an attack on the network (see appendices section 9.3). This shows attacks are not common within educational organisations. This could be due to the demographic of people within an educational institution or security implementations that the organisation has in place to prevent and stop attacks. Some of the questionnaires received reported as ‘none – as we know’, so they may not have received any attacks or they could have had an attack that is programmed to snoop for corporation data, however being an educational institution the data and information held at the school may not be of any use to the attacker. In this case the attack may be aborted therefore it would not be flagged up by the system.

One of the questions asked was does the school have an IT policy and only one school reported back they do not have an IT policy in place. As only one school reported back to
admit they do not have an IT policy in place, this is a very small response, however it is key to have an IT security policy in place to protect both the school and its pupils and staff.

37% of the questionnaires reported that they do not have IT training on best practices available for staff. This is a security threat for staff that are handling personal and confidential data. IT best practices are in place to train and help staff to use and handle data without compromising security.

A major concern is that only one questionnaire that came back reported that they have training for staff on security and best practices for using computing devices outside the organisation. 88% of the responses have no security training or best practices to use their own device outside the organisation whatsoever for staff. This can cause a great deal of security issues and threats with BYOD as devices brought into an organisation and connected to the network can cause security attacks, loss or copied personal information to an attacker via the connected device.

The questionnaires also found that 37% of the responses do not have IT training on best practices available for pupils. This can be another security threat as pupils using computers will need to know the IT policies and best practices to prevent attacks and security vulnerability such as viruses getting onto the network.

4.2.2. Security Methods Feedback

In the questionnaire the participants had the option to add additional information about how they have kept their security system secure or features that they believe are critical for a BYOD system. Some of the responses and analyses are below:

“From what I’ve seen BYOD is great when applied to older children, those sitting GCSE’s, A-Levels and at further/higher education environments but for younger children it is better stop BYOD and discourage it.”

The above response raises a security solution that can be an implemented into a BYOD network in educational institutions. BYOD is a policy to encourage students to bring their own devices to school due to the benefits (see section 2.3.2), however there can be different policies for each year group at the school to encourage older children to bring their portal digital device to school whereas younger students are discouraged. This will allow older children with more experience and more maturity to use the BYOD system. Also
discouraging younger student that do not need it will free up more bandwidth for the students that are using it.

“BYOD with younger pupils doesn’t just bring security risks, it brings risks of bullying at those disadvantaged, risks of safety to the pupils carrying devices back and forth to school and various other risks.”

The above response raises a valid security point for child safety. Younger school children carrying expensive computing devices to and from school bear the risk of this device being stolen, or even the risk of this device getting broken. Disadvantaged children who cannot afford devices to bring to school could also be bullied. More mature students are more likely to look after their devices and use it in a more appropriate way as they have GCSE and A-Level examinations coming up. The same concern was raised with another school:

“Principal’s policy [is] no mobile device to be seen or used in school. This is to prevent bullying from those with big brand names to those with cheaper budget devices or nothing at all. There is also the issue of insurance/theft.”

The school above raises the same issues about potential theft with a concern over insurances. Bullying could also be an issue for those who cannot afford laptops or ‘branded’ laptops.

“Although the guest network is technically open, /32 subnet mask restrictions are in place. Devices on the guest network cannot access others, and can only access DNS/DHCP ports on the domain controller, RDP/RemoteApp ports on the terminal server and web proxy ports on the gateway/filter – nothing else. The gateway intercepts initial web access requests and presents a domain logon portal to ensure appropriate filtering and tracking can be applied. Typing “remote.access” into a browser will present an RDP file for download to access a full logon session for authenticated users.”

As stated in the security feedback above the guest network is an open network, however devices connected to the guest network have limited access to the full internal network. This allows the system to keep a log of the activity of the devices connecting to the guest network and allows them browse the internet whilst protecting the internal network from attacks or unintentional threats.

“One of the few remaining security bugbears here is a lack of information filtering through to IT that students or staff are leaving the school, resulting in accounts remaining open as
potential attack or misuse vectors long after they should be. New organisations should apply ‘process mapping’ techniques early on to nip this in the bud before it becomes a major issue. Example process workflows attached to the e-mail (although we only have entry, not exit procedures so far).”

The feedback from above outlines a security vulnerability that can happen with new systems. A lack of communication between the employment/HR office and the IT helpdesk can cause user accounts being left open, which means that staff and pupils that have left the school can have access to the school’s system which is a security breach. Staff who have left on bad terms could use this security breach to deliberately misuse or copy/delete/edit data that they should no longer have access to. The feedback given also adds a solution to the security issue. The institution should adopt a process map for the IT department and the HR department to use in order to communicate with each other about the departure of staff and pupils, so that the IT department can add restrictions to the accounts or remove them.

“Get your group policies correct”

Another security recommendation from a school advised to get the security policies correct. It is important to get Group Policy correct to control the end user’s settings and capabilities. The group policy is usually split into two, user and computer configuration policy. It is key to have both settings correct in order to protect the internal network from users that are using their own devices.

### 4.2.3. Limitations

The questionnaire did have very low feedback compared to what was expected and to the number of questionnaires that were sent out to educational institutions. In this section this problem will be examined to identify possible reasons and how to solve this issue for future research in the area.

Survey Gizmo is a well-known online survey and questionnaire software company that has stated that response rates to questionnaires can fall below 2% if it is “less-targeted, when contact information is unreliable, or where there is less incentive or little motivation to respond.” (Fryrear, 2015). To make it more credible the questionnaire could have been on University of Derby headed paper to make the source more trustworthy. Logos used with permission from the University of Derby added onto the emails would also make the emails look more reliable.
The email addresses were gathered by visiting the local school’s website and then finding the email address, which is usually the reception or main office email address. Therefore the email asked the receptionist to forward the email to the IT department. This could be another reason for the low response rate as the email had to go through to two sets of barriers in the form of firstly the receptionist, and secondly the IT department before reaching an interested recipient. A possible solution could be not to email the questionnaire to the receptionist but to ask for the IT department’s email address.

As the questionnaire was attached to an email and sent to the schools, this caused a problem with trustworthiness of the email and the attachment. The above solution of adding logos and more sources to do with the university may have made it more trustworthy however the receivers may still have been dubious about opening attachments from unknown sources. This is because people are aware of phishing attacks where imposers send emails with attachments that contain viruses. A solution to this would be not using attachments (such as word documents) and instead using online surveys such as ‘SurveyGizmo’ (https://www.surveygizmo.com/) or ‘SurveyMonkey’ (https://www.surveymonkey.co.uk/), however using online software such as this costs money. Future research in this area may want to consider these options to gain greater feedback from educational institutions.

As the questionnaire asked a different range of security questions, it can also be a concern of the educational institutions to give away this information to people they do not know. This information could be used against the school if an attacker wanted to find out weaknesses within the organisation. One way to solve this is to make the source more trustworthy and limit the number of security questions that are asked.

Previous research into the security aspect of BYOD in educational institutions is very limited and the main research discussed in section 2 of this report focused on the general threats and security of BYOD. Therefore the outcome of the questionnaires and feedback were going to be truly unknown. The issue was that the questionnaire covered a wide range of questions spanning across different areas, this had the negative effect of the questionnaire asking for too much information and being too long, as the feedback in section 4.2.4 suggests. If further work is to commence in this area, the results of the security concerns that have been identified as common recurrences can be inspected, reducing the range of questions and the number of question, which in turn may increase the number of responses.
The timing of the questionnaire to the schools could also be an issue. In the UK the school year starts in September and ends in July therefore throughout these dates the school is in full operational mode and can be very busy. Therefore the idea timing could be just before or during the summer holidays.

The incentive given to educational institutions was that the recommendations produced by this report would be sent to the IT technicians that took part in the survey. However to have a greater incentive for IT technicians to fill out the questionnaire in the future, an in depth detailed abstract could be attached to the email explaining the consequences of not having a secure BYOD system and why this research is important.

4.2.4. Feedback

Feedback was requested from those who took part in the questionnaire on areas of improvement and also to help discover why the response rate may have been so low. An extract of a response from one of the schools is below:

“The questionnaire has taken 40 minutes to complete rather than the 5-10 suggested and I had to obtain permission from my manager and the school’s leadership team.”

The reason as suggested in the section 4.2.3 as well as above, is that there may have been too many questions asked, this again been discussed in section 4.2.3 which says that due to previous research in the area being limited the outcome was unknown. As a result the range of questions asked was not concentrated on any particular area. In the future, amending the questionnaire so it focuses on a certain security aspect, as well as reducing the number of questions could increase the number of responses.

4.2.5. Future solutions

The sections 4.2.3 and 4.2.4 above have identified limitations and problems that may have caused the low turnout in responses to the questionnaires. Further research in this area may want to consider using survey or questionnaire software even if it costs money to do so. Using logos of the organisation on whose behalf you are doing the research will make the source more trustworthy. Emailing the technicians direct by getting their email address from the reception rather than trying to email the questionnaire to the reception and asking them to send it onto the IT department, would be more effective. Trimming down the questionnaire and only focusing on the key security issues that have been flagged up by this report, will
make the questionnaire less time consuming which in turn should increase the number of responses.

4.3. Conclusions

Section 4.2.1 has identified some security vulnerabilities that have a common occurrence with educational institutions that need addressing in order to make the organisational BYOD system more secure. The main security concern is that 88% of those who responded do not train their staff or have best practices in place for staff to use their own devices outside the organisation, which is a security threat that will be discussed in section 5. Other security issues include some schools not having IT best practices for both students and teachers on how to use the computing system within the organisation; this will also be discussed in section 5.

Section 4.2.2 outlined security feedback to help with the final recommendations which are discussed in the later sections. Finally section 4.2.3 outlined limitations with the report and improvements and recommendations for future work in this area.
5. Discussion

5.1. Introduction

This section will be looking at the issues that have been identified in the research above and use the findings in the literature review to back up the arguments. From this different security methods will be identified and examined for the final recommendations.

5.2. Training

An area that has been identified that is a concern both for systems with and without BYOD which affects the network security and children’s wellbeing, is the lack of training for staff members in the use of devices outside the organisation. Section 4.2.1 has identified this issue as it shows that 88% of the responses do not have training for staff on how to use computing devices outside the organisation, which is both a problem for networks with and without BYOD. The issues and problems will be discussed in the next section.

5.2.1. Issues

They are many issues with staff having a lack of training which affects both BYOD and non-BYOD educational institutions: BYOD are affected as staff are able to download data and personal data onto their own device and Non-BYOD devices are still able to download data and personal information via email or memory sticks, which many people tend to do with or without permission as identified in Section 2.7.2.

With data, especially personal data such as child records, if the device that it is downloaded to do not have adequate security implemented then it makes it easier for attackers to gain access to the laptop and steal information. Mis-configured or poorly configured synchronised settings to online storage devices (Dropbox, OneDrive, Google Drive) can, unknowingly to the user, copy the personal information to the cloud which could break the organisational policy and make it easier for others to gain access to the information.

Staff with little computing knowledge who use their laptops on various different WiFi connections could create security vulnerabilities if they connect to unprotected open networks when downloading or uploading personal information. Other security issues can be down to
computer illiterate staff members being exploited by attackers via wireless attacks, for example MITM (Man-In-The Middle) or eavesdropping attacks. This concern was also echoed from an ICT manager in schools 4, however staff are able to email the IT department with their concerns (see appendices section 9.4).

Other security issues arise with lack of security awareness of staff members using their own laptops with personal data on them such as not having an updated anti-virus software to protect the laptop from viruses and other attack methods, or staff not understanding phishing methods. Laptops with weak security authentication make it easier for access to be gained to data on lost and stolen devices. Lost and stolen device are quite common as identified in section 2.4.

5.2.2. Solutions

The solutions to resolve the issues above would be to offer relevant information, training or guides on IT and security best practices in order to keep devices secure. The information should include some of the following guides:

- Installing, maintaining and updating anti-virus software. This is paramount to prevent and identify attacks on the machine. Staff should be trained or informed how to perform the basic virus scans and advised to perform these scans on a regular basis.

- Understanding wireless security. The staff that have portable devices that travel to various locations should be shown what icons to look for to identify whether the wireless connectivity is secure and how secure. Staff should also be aware and able to identify open wireless networks and their threats to eavesdropping attacks when uploading and downloading data.

- Identifying attacks. The staff should be able to identify phishing emails and websites to prevent attacks or sending information to fraudulent people. The identification of HTTP and HTTPS in browsers will help the staff identify when a website is secure.

- Configuration and settings. The computing device should be configured with a strong password to prevent attackers gaining access to a lost or stolen device.
Staff should be taught how to add and change a password and be recommended to use strong passwords for all their devices and logins.

- **Procedures.** Staff should have access to guides and best practices to follow in order to keep their computing systems secure. For devices that are lost, a procedure should be in place for the protocol on what they should do. The IT department will need to know in order to stop the device gaining access to the organisation’s network and accessing data.

In order to provide staff with the best practices and the different security protocols there are many different methods. The methods are listed below and explained:

- **Paper based booklet** can be issued to staff members on the security best practices and computing procedures. Paper based booklets are handy for staff to take home with them or to keep the booklet with their laptop. Also staff with little computing knowledge will be able to follow the steps by looking at the booklet and mimicking them on their own device. However a booklet alone relies on the staff to read and understand it.

- **Email booklet,** can be emailed to new staff members and to all staff members on an annual basis. It should contain the security best practices which has the advantage of saving paper. However as many staff members may get many emails every day, the emailed booklet may be lost in the inbox among a lot of other emails. Same problem exists as with the paper booklet in that it requires the staff to read the material and to understand it.

- **Online booklet** can be available for staff to access the different security best practices and procedures via the internet. This has the advantage of easy access as links to the online booklet can be on the landing page and on the school’s website. Any changes to the security best practices can be updated instantly. Links to other useful material and software can be added to the online booklet (for example links to anti-virus software). The staff must be aware of this and know how to find it. It also requires them to read the information and understand it.

- **Training** can be used to demonstrate and explain to the staff members the security best practices and procedures. Training can help staff members
understand and ask questions to further their understanding. The training can be done externally, however internal training by the IT schools helpdesk can be more convenient and cheaper. Step by step demonstrations can be shown to the staff to increase their knowledge and understanding. Explanations via audio, visualisation and hands on tend to work better than text (Jewitt, 2008). As the above training methods require the staff member to read and understand the booklet, using this training method they are more likely to take in the information and any confusion or misunderstanding can be dealt with by the trainer.

- Tests can be used to check the understanding of the security best practices of the staff members. Rules can be added such as, ‘in order for staff to use their own device they must pass the test’. The tests can be an effective way to ensure the staff members understand the booklets and/or the training as mentioned above.

The educational institution could have a policy in place that in order for staff to use their own machines, it must be checked by the IT Helpdesk department to ensure the security settings. However, this will increase administrative overheads and can be impossible to implement and upkeep due to staff time involved and staff using unchecked devices without the helpdesk’s knowledge.

5.3. **ICT Policies**

The questionnaires from the schools outlined a positive response to having an ICT policy in place, as only one school admitted to not having an ICT policy in place. In the literature review, section 2.4 outlines the importance of having an ICT policy and this is backed up by some of the schools security feedback given in section 4.2.2. Even though the majority of schools have got an ICT policy in place it is important that it is up-to-date and efficient.

The ICT policies tend to cover the training, security and procurement and should be signed and agreed by both staff and students before using the IT equipment. The policies should be regularly reviewed to ensure they meet the objectives of the organisation. Online handbooks are available such as ‘The APC ICT Policy Handbook’ (Souter, 2009) and ‘ICT Policy: A Beginner’s Handbook’ (Nicol, 2003) that provide an in depth guide on creating ICT policies for organisations.
Two policies have been added to the appendices that were sent back with completed questionnaires. School 5 has a procedure for lost, stolen or replacement devices for both school computing devices and staff personal computing devices, stating that it must be notified to the IT department. However school 8 does not have this written in the documentation but otherwise both schools policies are well written and in depth. School 8 policies are split into two, ‘IT Policy for Staff’ which gives an overview of the policies and refers readers to the second document ‘IT Responsible User Guide’. The ‘IT Policy for Staff’ is clearly dated however the second document ‘IT Responsible User Guide’ is not dated which can cause issues in the future as it is updated, therefore it needs dating. The second school 5 dates the policy document and gives a date of next policy review of 2018 (3 years after the approval date). The date does not state that it is provisional which can cause confusion if it has to be updated sooner. New technologies or changes to the schools network and/or system may happen before the date, resulting in the need of the ICT policy to be updated; therefore the next policy review does not need to be printed onto the sheet. In the appendices there is a range of different ICT policies covering a range of IT, BYOD and media aims, usage, security and rules, that was sent in with the questionnaires. The actual policy format and needs will vary depending on the needs. The policy documents can be found at Appendices section 9.9 – 9.14 of this report.

### 5.4. Creating and deleting users

Section 4.2.2 identified that creating and deleting user accounts can be an issue due to the internal process. When new staff or pupils start school the IT department could be rushed into making a user account due to lack of previous communication between HR and the IT department which can cause security flaws. There needs to be a set procedure to ensure the right IT policy and settings are applied to the new user, as well as giving any training if necessary and ensuring that the right documentation is signed by the user. School 3 has sent their process flow for adding a new user to the system. The acknowledgment of the procedure documentation from both the IT department and HR will create a smooth process of adding new users to the system in a sustainable way to avoid any security issues.
Figure 1 – shows School 3 process of adding a new staff member to the school (Timms, 2016).

Figure 2 – shows School 3 process of adding a new student member to the school (Timms, 2016).

In the final recommendations the procedures above will be adopted for a template for other schools to use. A process flow will also be added to the recommendations for the departure of both staff and students as this is important to avoid accounts being left open which is a security issue as staff who have left on bad terms could use this security breach to deliberately misuse or copy/delete/edit data that they should no longer have access to.

5.5. Conclusion

This section has outlined and discussed in depth different solutions to the problems identified in section 4 and explained why they are important. The solutions identified, along with
information found in the literature review (section 2), will be documented in the recommendations below.
6. **Recommendations**

This section will outline the additional recommendations for educational institutions to consider in the future when implementing a BYOD system into their network. For educational institutions that have already have a BYOD system implemented, these recommendations can still be useful as certain tweaks to their existing security network maybe ideal to further protect the network.

6.1. **Planning and Implementation**

This report has outlined some additional considerations that an educational institution may want to consider when planning and implementing a BYOD solution.

6.1.1. **Network and wireless**

For any organisation to implement BYOD into their current system they will have to bear in mind that BYOD means that almost certainly more devices will connect to the network. With more devices on the network this will increase the network overheads and bandwidth. Many wireless BYOD solutions will come with monitoring tools, but even so these will only give analyses and data for the wireless aspect and will only come into effect after the implementation.

Before implementing BYOD it is advisable to gather network statistics to see if the current network will be able to handle the extra workload and bandwidth. Many networking devices (routers, switches) and servers will have their own monitoring system to measure performance and availability. However many network management tools will help consolidate all the devices performance and status statistics into a single software, making it easier to manage. There are many network management tools available and Spiceworks (http://www.spiceworks.com) is one free network monitoring tool that has proved to be effective and is therefore recommended by this report (SpiceWorks, 2016).

Schools without a wireless system in place can start from a clean slate. Schools with wireless systems in place, can use the existing infrastructure and extend from this. There are wireless tools that help organisations plan where to place wireless AP such as Ekahau (http://www.ekahau.com), which is a wireless site survey and planning software that supports
wireless IEEE802.11 a, b, g, n and ac (Ekahau, 2016). Wireless site survey and planning software tools can be expensive, adding to the total cost. Planning can be done by using a measured site map and working out the range of the wireless AP taking into consideration for example the physical environment such as walls. This method is less accurate however is cheaper than using wireless planning tools. Certain areas may need more than one AP if there is going to be a high number of wireless devices and bandwidth required. The following formula can be used to work out how many APs are needed:

\[ T = ND \times AP \]

note: \( AP \% = \frac{RBW}{MBW} \)

MBW = Minimum Bandwidth required for each device

RBW = Real bandwidth of the Device*

ND = Number of Devices

AP = Airtime Percentage [%]

T = Total number of radios needed. For every 100% another AP is needed.

*TCP/IP throughput is usually 40-60% of the maximum capable speed.

(Formula source: (Alternetworks Corp, 2014 ))

If an analysis of the network data and performance statistics suggests that the network does not have the capability to handle the extra workload of more devices using the network, then upgrading the existing network infrastructure will have to be applied. The upgrading costs for a network to have a significant and adequate capacity to handle a BYOD solution will differ depending on many variables, however as (Capgemini Consulting, 2013) report shows many organisations benefit financially after the implementation of BYOD. This is illustrated in the pie chart shown below:
Figure 3 – shows the Percentage of Respondents According to Impact of BYOD on Expenditure (Xigo and CCMI, 2021).

As shown in Figure 3, many organisations benefit in the long term from BYOD, as 67% of organisations saw financial benefit after BYOD implementation compared to 24% that saw an increase in expenditure (9% saw no change in expenditure).

Once the organisation has established that there is significant network capacity to handle the extra traffic then it can proceed onto the next stage of planning and implement a BYOD solution.

6.1.2. Gathering feedback and pre-installation

A BYOD solution comes in different shapes and sizes, therefore gathering information before implementing a solution is key. Different sets of people will be affected by the implementation of the BYOD and will need to be consulted and their views to heard to help paint a picture on how the BYOD should work and function. An ideas group of people that should be approached are the following:

- Teachers – teachers that want to use the BYOD in classrooms or use eLearning technologies may determine the location and/or the amount of Wireless APs needed in certain locations. Consulting with staff members before the installation process may result in staff members researching different eLearning technologies that they may want to use which will help with the planning and installing of the BYOD solution.
• Pupils – The input from students could help with the planning. Students can suggest different eLearning technologies they would like to use and even trial some of these technologies. Certain student focus groups can be established to trial the technologies, help other pupils and staff members. As it requires time from the pupils taking part, an incentive may be needed to attract students.

• Head Teacher – The Head Teacher should be notified as it is a big change in the network and how the school runs. The Head Teacher should have the final say on whether to go ahead with the system or not as it can have implementations that can affect the school. The Head Teacher can also have input into the solution which can help with the planning.

• Parents, community groups and board members – Parents feedback and support should be welcomed. Parents may have concerns with BYOD and students bringing computing devices to school. The community and the backers of the school, especially now the UK is moving towards an academy system may help sponsor or support a BYOD solution. The BYOD system could be seen as a good investment especially to those schools that let out their premises. The school’s board members can express a range of views and any concerns about a BYOD system.

6.1.3. Implementation and post installation

The implementation and installation of BYOD can be very difficult but the correct planning and rollout will smooth the process and will create less overheads and costs for the future. The BYOD should be flexible and should consider future extensions that may happen to the network or the physical infrastructure of the school. Before a BYOD goes live, the security aspects need to be addressed which will be discussed in section 6.2.

Once the BYOD system has been installed and is live, this report advises an initial trial of the BYOD only with certain departments (Math teachers, English teachers) or groups (year groups, form groups). This will allow the BYOD system to be tested without any major interruption in teaching and learning. After the BYOD system has been tested, then it can be slowly rolled out to ensure the network can handle the increased workload with regular network status and performance tests and analyses.
Post the BYOD system having gone live, frequent baseline checks should be performed to check network performance and ensure BYOD is functioning correctly. Many wireless BYOD solutions come with monitoring software to help check performance of the wireless network and some BYOD solutions allow WiFi mapping to check the wireless coverage and strength of the wireless network. To get an accurate wireless map of the network, it is advisable to use the WiFi mapper and to use a WiFi analyser software to determine the actual strength of the signal. Software such as ‘Spectrum Analyzer’ from Ekahau (http://www.ekahau.com/) offers in depth wireless mapping which can be done via uploading a map and walking around the site with a wireless device (Ekahau, 2016). However this can be costly, and a cheaper alternative would be using free software like the “Wifi Analyzer” (http://wifianalyzer.mobi) that can be used by technicians walking around the site into areas where BYOD is needed and test the wireless signal. By doing this the IT technicians then can analyse the data and tweak the wireless network if need be to improve the performance and availability.

Feedback from staff and students can be used to gather information of the end user’s experience of the BYOD system. This will help troubleshoot any problems or aid any adjustments that may be needed to increase performance and experience. Feedback could also help with future performance or assess eLearning software the school may want to trial.

6.2. Security

This section will discuss the security aspects of the BYOD. The main focus of this section is to highlight additional security measures that an education institution should consider on top of the traditional BYOD security measures. Children’s wellbeing should be at the frontier and a high priority of the security implementations at an educational institution, especially when adopting a BYOD solution as it increases the security vulnerabilities if not installed correctly.

6.2.1. Overview

The school should already have anti-virus software deployed across the network and run regular checks. However machines that are connecting to the internal network and handling personal data should have an up-to-date anti-virus software. The personal machine should also perform regular security scans for any malicious software. The existing wireless system or the new wireless system should use the WPA2 encryption standard as it is most secure wireless system.
Creating VLANs and subnets for the different groups is advisable to increase both security and network management. An example would be having a VLAN and a subnet group for staff to allow them access the internal network (allow them to perform registration and performance tasks for example on their own machine) however then having a separate VLAN and subnet for pupils and staff that do not need access to the internal network or the same resources.

Depending on the BYOD solution setup, if the setup is as advised above with different VLANs and subnets, then different groups will be routed differently. It is important they still have a firewall and a proxy in place when communicating with devices and with the outside world. The firewall should stop unwanted traffic and prevent attacks. As an educational institution has a responsibility for the child’s wellbeing the report instructs them to have a filtering proxy server in place between the connection of any devices (schools and personal) to the internet. The filter role is to stop users accessing unapproved websites. There are many different proxy and filtering solutions available. If budget for the project is limited then there are free solutions available; a recommended example would be using a Linux ‘OpenSquidBox’ (https://sourceforge.net/projects/opensquidbox/) which is a pre-configured Squid Proxy Cache Server (Unveiltech, 2015) which is compatible with ‘DansGuardian’ (http://dansguardian.org/) which is an Open Source web content filter which runs in Linux (DansGuardian, 2011).

Many BYOD solutions will have monitoring capabilities and security features to help protect the system (Ruckus, 2016). Using IDS/IPS (Intrusion Detection/Prevention Systems) is advisable to help detect malicious activity, rogue devices or equipment trying to gain access onto the network. Most wireless APs such as Cisco’s 1000 series or the current ZoneFlex Ruckus system (Ruckus, 2016), automatically detect and collect information on rogue APs, detected by its managed access points which then issue a warning to the IT department, which includes the location of the rogue AP (Cisco, 2006).

An optional way of protecting the network and devices in a BYOD network is to use MDM (mobile device management). MDM is a piece of software that manages, monitors and supports mobile devices on the network. However each device will need to be allowed onto the network, therefore this is a good idea to manager the devices that want to gain access to the internal network and allow the rest of device to have internet access only. In a school with potential 100’s/1,000’s of students connecting their devices it can become impossible to manager.
6.2.1. Policies and best practices

Schools should already have an ICT policy in place. When implementing BYOD the policy should be updated to include the policies for the BYOD system. The policies are needed to achieve best value and to reduce risk. The ICT policy or AUP (Acceptable Use Policy) is in place to cover different aspects such as the correct use of the ICT equipment, security, training and procurement and should be reviewed on a regular basis. In the questionnaire that was sent out to the schools all bar one had an ICT policy in place, therefore the establishment of an ICT policy within educational institutions is not a major issue, however reviewing and updating the policy is advisable. A BYOD policy template can be downloaded via Honeywell Enterprise ([http://info.enterprisemobile.com/byod-policy-template.html](http://info.enterprisemobile.com/byod-policy-template.html)), however tweaks to the template will need to be considered for each different institution to meet their needs. A range of different school’s ICT policies have been added to the appendices (section 9.9 – 9.14) and have been scrutinised in the discussion section (section 5.3) of this report.

Online handbooks are available such as ‘The APC ICT Policy Handbook’ (Souter, 2009) and ‘ICT Policy: A Beginner’s Handbook’ (Nicol, 2003) that provide an in depth guide on creating ICT policies for organisations.

In educational institutions, younger school children carrying expensive computing devices to and from school bear the risk of this device being stolen, or even the risk of this device getting broken. Therefore it is advisable to have different policies for each year group at the school to encourage older children to bring their portal digital device to school whereas younger students are discouraged. This will allow older children with more experience and more maturity to use the BYOD system. Also discouraging younger student that do not need it will free up more bandwidth for the students that are using it.

This report found that 37% of schools which took part in the questionnaire did not have a best practice guide for using the IT system within the school (see section 4). Best practice and informative documents should be issued to staff members who will be using the BYOD. The best practice documents should cover a range of procedures for using computing devices inside and outside the organisation. A policy and best practice procedure covering the loss of school and personal devices should be reported to the IT department should be added to the policy document. This is due to the laptop having outside access to the school’s network and may contain confidential information that may affect the school. The correct use of using a device outside an organisation is also important to decrease the security vulnerabilities. This
This report advises that online guides and informative information should be available to staff. A link to the documentation should be emailed out on an annual basis and to new staff members. An online document is easier to access, maintain and change.

This report in section 4 found that 88% of the responders have no security training or best practices whatsoever for staff to use their own devices outside the organisation. This is an issue for staff using their own personal device on the BYOD and accessing confidential data. Therefore for staff who are using their personal device on the BYOD network it is highly recommended that documentation and best practices are available that cover the following:

- Installing, maintaining and updating anti-virus software. This is paramount to prevent and identify attacks on the machine. Staff should be trained or informed how to perform the basic virus scans and advised to perform these scans on a regular basis.

- Understanding wireless security. The staff that have portable devices that travel to various locations should be shown what icons to look for to identify whether the wireless connectivity is secure and how secure. Staff should also be aware and able to identify open wireless networks and their threats to eavesdropping attacks when uploading and downloading data.

- Identifying attacks. The staff should be able to identify phishing emails and websites to prevent attacks or sending information to fraudulent people. The identification of HTTP and HTTPS in browsers will help the staff identify when a website is secure.

- Configuration and settings. The computing device should be configured with a strong password to prevent attackers gaining access to a lost or stolen device. Staff should be taught how to add and change a password and be recommended to use strong passwords for all their devices and logins.

- Procedures. Staff should have access to guides and best practices to follow in order to keep their computing systems secure. For devices that are lost, a procedure should be in place for the protocol on what they should do. The IT department will need to know in order to stop the device gaining access to the organisation’s network and accessing data.
However the documentation alone requires the staff members to read and understand the document, therefore it is advisable to have a training session and tests for staff to complete before they are allowed to bring their own device and use the BYOD facility. The training will be discussed in the next section.

6.2.2. Training and Tests

As discussed above (section 6.2.1) the documentation of the best practice for both inside and outside the organisation is necessary however it requires the user to read and understand the documentation. Therefore training is an optional recommendation that educational institutions can adopt to help staff understand the policies and best practices of using computing devices both inside and outside the organisation. Any confusion or not understanding any of the best practices can be dealt with, in the training session. Training sessions can be done externally, however internal training by the IT department will cost less and the IT department will understand the nature of the organisation and its needs.

Testing staff is a good way to test their knowledge of the best practices and the ICT policies of the schools. The test should include security questions to ensure the staff members who wish to use their own device on the network have an adequate knowledge and understanding. Training does not need to be accomplished in order to take the test as the online documentation that are available may be sufficient for some members of staff. It is advisable that staff must complete the test before using their own device on the network.

6.3. Procedures

The communication between the HR department and the IT department has to be efficient in order to inform the IT department of new starters (staff and pupils). Lack of communication between the two departments can cause issues such as adding the staff into the wrong GPOs, not receiving or understanding the ICT policies and missing out on ICT training. These problems can also be caused if the ICT helpdesk has insufficient notice time to create the accounts. These problems have been backed up from a school’s security feedback (see section 4). A solution given by the school is to have a process flow for creating new staff and pupil members. In order for the process flow diagram to work all departments involved should adhere to it. The school sent their process flow diagrams (see figure 1 and 2) and this report has used the diagram to create its own template for schools to use, however schools will need
to tweak the diagram to make it fit their organisation structure. The process diagram can be found below:

Figure 4 – shows a template process flow for adding a new staff member to an educational institution.

Figure 5 – shows a template process flow for adding a new pupil member to an educational institution.

As can be seen from both figure 4 and 5 the signing of the ICT policy document is included in the diagram. Some schools have the terms of use on the logon screen which states by logging onto the computer you agree to the AUP/ICT policy agreement. However staff and pupils using their own devices will not have the same log on screen stating this, therefore it is important to get the staff and pupils to sign the AUP/ICT policy documents.
Wireless aspects of a BYOD solution have the ability of allowing users to gain access to the network when they are offsite. This is dependent on the wireless strength and the size of the premises. However due to this possibility and along with VPN and E-mail accessibility, it is important that the account is disabled to ensure access cannot be gained from users outside the organisation. If there is a lack of communication between the line manager and/or HR department and the IT department then this can cause security vulnerabilities as accounts can be left open and staff who have left on bad terms could use this security breach to deliberately misuse or copy/delete/edit data that they should no longer have access to. Therefore using a similar flow diagram as above, the report has created a flow diagram (see below) for disabling accounts for when staff leave the organisation.

![Flow Diagram for Disabling Accounts](image)

Figure 6 – shows a template process flow for removing a staff member from an educational institution.
Figure 7 – shows a template process flow for removing a pupil from an educational institution.

Note: The diagrams above are templates and will need to be adapted for each organisation and their procedures. However the diagrams are there for an example and this report recommends educational institutions to create their own.

6.4. Conclusion

From the literature review and the research findings of security issues that come with BYOD, this report has provided some additional recommendations for educational institutions that they should consider when implementing a BYOD solution to help protect its network, confidential information and children’s wellbeing.
7. Future work

This section will give some recommendations for future work that can be considered for more research in this area. Future research that wants to gather information via questionnaires should look at the limitations (section 4.2.3) and solutions (section 4.2.5), in order to increase the response rate from schools. With a greater response rate the findings will be more valid. Future research could look into the different types of BYOD solutions available and which one could be best suited for educational institutions. It could also consider researching into how effective BYOD is to educational institutions and whether it increases productivity and/or reduces the computing budget of the school.
8. References


Available at: http://byod.us/cost-effective/
[Accessed 15 May 2016].


Available at: http://dansguardian.org/?page=whatisdg
[Accessed 17 May 2016].


Available at: http://www.ekahau.com/wifidesign/spectrum-analyzer
[Accessed 17 May 2016].

Ekahau (2016). Wi-Fi Planning and Site Survey and Planner. [Online]
Available at: http://www.ekahau.com/wifidesign/ekahau-site-survey
[Accessed 17 May 2016].

Evans, D. (2015) What is BYOD and why is it important? The opportunities and risks of people using their own devices at work. [Online]
Available at: http://www.techradar.com/news/computing/what-is-byod-and-why-is-it-important--1175088
[Accessed 20 January 2016].

EY Foundation, 2013. Bring your own device: Security and risk considerations for your mobile device program, s.l.: EY Foundation.


Available at: [https://www.ruckuswireless.com/products/access-points/zoneflex-indoor](https://www.ruckuswireless.com/products/access-points/zoneflex-indoor) [Accessed 18 May 2016].

Available at: [https://www.ruckuswireless.com/technology/byod](https://www.ruckuswireless.com/technology/byod) [Accessed 18 May 2016].


SpiceWorks (2016) *Spicin’ IT up all workday long*. [Online]


Webroot (2014) *MOBILE SECURITY: Fixing the Disconnect Between Employer and Employee for BYOD (Bring Your Own Device)*, s.l.: Webroot.

Xigo and CCMI (2012) *Mobility Temperature Check: Just How Hot Is BYOD?*, s.l.: CCMI.

9. Appendices

Section 9.1 – 9.8 of the appendices has the questionnaires that were sent in with the security feedback.

Section 9.9 – 9.14 has the school’s policy documents that were sent in and any other documentation that the school thought it was important to send.

The school names have been removed as stated in section the Research Methodology (section 3) of this report.

Information in the below section could also help with future work in this subject.
9.1. **Questionnaires from school 1**

**KIRK KUS – UNIVERSITY OF DERBY – FINAL YEAR PROJECT QUESTIONNAIRE**

20 January 2016

**THE SECURITY EFFECTS OF BRING YOUR OWN DEVICE (BYOD) IN SCHOOLS:**

Questionnaires for educational institutions that have **NOT** got BYOD installed.

1. Information on the project: My final year project at the University of Derby is on the security implications of Bring Your Own Device for educational institutions. My research will help build a report on BYOD recommendations that schools should consider to protect the security of children’s information and prevent it from falling into the wrong hands. All responses will be kept in confidence, more details can be found on the consent documents that were attached to the questionnaire.

**QUESTIONNAIRE.**

1. **Your details.**

   A) Position: Systems Technician
   
   B) Date: 20th February 2016

2. **School information:**

   A) School’s name: 

3. **BYOD information:**

   A) Are you planning on installing BYOD in the near future: 
   
   Yes □
   
   If Yes Please answer B) and move onto D)
   
   No □
   
   If No please go to question C)

   B) When are you planning to install BYOD in your organisation:
   
   Within a month: □
   
   1 – 3 months’ time: □
   
   3 – 6 months’ time: □
   
   6 months’ – 1 year □
   
   1 – 2 years □
<table>
<thead>
<tr>
<th>Question</th>
<th>Response</th>
</tr>
</thead>
<tbody>
<tr>
<td>C) If A = Never, please can you give details why you are not planning to install BYOD:</td>
<td></td>
</tr>
<tr>
<td>At the end of this academic year the school is being closed for good by the local authority.</td>
<td></td>
</tr>
<tr>
<td>The school intake and catchment area is very deprived with high pupil premium percentage so students wouldn't necessarily have the devices at home.</td>
<td></td>
</tr>
<tr>
<td>D) Are there security issues with BYOD that are of concern to you:</td>
<td></td>
</tr>
<tr>
<td>Duty of care - unable to properly monitor students on their own devices.</td>
<td></td>
</tr>
<tr>
<td>Potential for viral infection etc.</td>
<td></td>
</tr>
<tr>
<td>Unauthorised software being used on the school networks potentially for malicious use.</td>
<td></td>
</tr>
<tr>
<td>E) Does your organisation have a wireless system:</td>
<td>Yes</td>
</tr>
<tr>
<td>No</td>
<td></td>
</tr>
<tr>
<td>If No please go to question J)</td>
<td></td>
</tr>
<tr>
<td>F) What type of wireless security does the organisation network have:</td>
<td>None</td>
</tr>
<tr>
<td>WEP</td>
<td></td>
</tr>
<tr>
<td>WPA</td>
<td></td>
</tr>
<tr>
<td>WPA2</td>
<td>X</td>
</tr>
<tr>
<td>G) How many different devices connect to the wireless network on average in a day:</td>
<td>40 approx.</td>
</tr>
<tr>
<td>H) Have you ever had an attack on your network, if so please give details.</td>
<td>Not knowingly.</td>
</tr>
<tr>
<td>If no, please go to question J)</td>
<td></td>
</tr>
<tr>
<td>I) How was the attack dealt with:</td>
<td>N/A</td>
</tr>
<tr>
<td>J) Are there any other security information you like to share for new organisations:</td>
<td>Schools should be mindful of permissions on school networks and locations of sensitive data in order to restrict access to it. Regular, secure backups should be taken in order to provide disaster recovery.</td>
</tr>
</tbody>
</table>

4. Policy and training information.

A) Does the school have an IT Policy in place: | Yes | X |

No |
### B) If possible can you copy the policy into the box:

<table>
<thead>
<tr>
<th>C) How are staff and pupils informed of the policy and any changes in it?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Staff are trained and informed via CPD and distribution of policy via email and physical copies distributed for staff to read and sign, logs kept of who has signed.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>D) Is IT training on best practices available to staff:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes ✔️</td>
</tr>
<tr>
<td>No</td>
</tr>
</tbody>
</table>

Staff are provided with an AUP that contains best practice and I provide ad hoc advice and training especially if any breaches of best practice occur.

<table>
<thead>
<tr>
<th>E) Is training for staff on security and best practices for outside the organization available:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
</tr>
<tr>
<td>No ✔️</td>
</tr>
</tbody>
</table>

Advice is available on request and often I can provide literature or websites for staff to look at regarding their concern.

<table>
<thead>
<tr>
<th>F) Is IT training on best practices available to pupils:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes ✔️</td>
</tr>
<tr>
<td>No</td>
</tr>
</tbody>
</table>

The students do courses as part of their IT lessons on Online Safety, IT use and other related topics.

<table>
<thead>
<tr>
<th>G) Is there any further information you would like to share that can help me with my project please:</th>
</tr>
</thead>
<tbody>
<tr>
<td>From what I’ve seen BYOD is great when applied to older children, those sitting GCSE’s, A Levels and at further/higher education environments but for younger children it is better stop BYOD and discourage it. BYOD with younger pupils doesn’t just bring security risks, it brings risks of bullying at those disadvantaged, risks of safety to the pupils carrying devices back and forth to school and various other risks.</td>
</tr>
</tbody>
</table>

---

Thanks for taking part in the questionnaire. Your time and information is much appreciated.

Please sign the form at the bottom so I can use the data provided.

Kirk Kus – University of Derby

Email address: K.Kus1@unimail.derby.ac.uk
9.2. **Questionnaires from school 2**

---

**KIRK KUS – UNIVERSITY OF DERBY – FINAL YEAR PROJECT QUESTIONNAIRE**

**20 January 2016**

**THE SECURITY EFFECTS OF BRING YOUR OWN DEVICE (BYOD) IN SCHOOLS:**

Questionnaire for educational institutions that have **NOT** got BYOD installed.

Information on the project: My final year project at the University of Derby is on the security implications of Bring Your Own Device for educational institutions. My research will help build a report on BYOD recommendations that schools should consider to protect the security of children’s information and prevent it from falling into the wrong hands. All responses will be kept in confidence, more details can be found on the consent documents that were attached to the questionnaire.

---

**QUESTIONNAIRE.**

1. **Your details.**

<table>
<thead>
<tr>
<th>A) Position:</th>
<th>Head of Computing</th>
</tr>
</thead>
<tbody>
<tr>
<td>B) Date:</td>
<td>29/2/2016</td>
</tr>
</tbody>
</table>

2. **School information:**

<table>
<thead>
<tr>
<th>A) School’s name:</th>
</tr>
</thead>
</table>

3. **BYOD information:**

<table>
<thead>
<tr>
<th>A) Are you planning on installing BYOD in the near future:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes ✅</td>
</tr>
<tr>
<td>If ‘Yes’ Please answer B) and move onto D)</td>
</tr>
<tr>
<td>No ✅</td>
</tr>
<tr>
<td>If ‘No’ please go to question C)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>B) When are you planning to install BYOD in your organisation:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Within a month:</td>
</tr>
<tr>
<td>1 – 3 months’ time:</td>
</tr>
<tr>
<td>3 – 6 months’ time:</td>
</tr>
<tr>
<td>6 months – 1 year:</td>
</tr>
<tr>
<td>1 – 2 years:</td>
</tr>
</tbody>
</table>

---

1
<table>
<thead>
<tr>
<th>Question</th>
<th>Answer</th>
</tr>
</thead>
<tbody>
<tr>
<td>C) If A = Never, please can you give details why you are not planning to install BYOD:</td>
<td>2 years + ☐ Never: ☐ If other please state: [ ]</td>
</tr>
<tr>
<td>D) Are there security issues with BYOD that are of concern to you:</td>
<td>We are currently changing our whole network and server infrastructure, therefore security concerns are being addressed as we do this. Overall we have found that our current system is too secure and impacts on network performance.</td>
</tr>
<tr>
<td>E) Does your organisation have a wireless system:</td>
<td>Yes ☑ No ☐ If No please go to question J)</td>
</tr>
<tr>
<td>F) What type of wireless security does the organisation network have:</td>
<td>None: ☐ WEP: ☐ WPA: ☐ WPA2: ☐</td>
</tr>
<tr>
<td>G) How many different devices connect to the wireless network on average in a day:</td>
<td>This is a new wireless system that is still in the testing phase, however we expect around 10-20 devices a day. We are a very small school and currently only some staff will be using the wireless system.</td>
</tr>
<tr>
<td>H) Have you ever had an attack on your network, if so please give details:</td>
<td>No. If no, please go to question J)</td>
</tr>
<tr>
<td>I) How was the attack dealt with:</td>
<td></td>
</tr>
<tr>
<td>J) Are there any other security information you like to share for new organisations:</td>
<td>Do not over do security, it is important but you need to remember that you are a school not a high security government installation... security is important but don’t over do it and lock everything down!</td>
</tr>
</tbody>
</table>

4. Policy and training information:

<table>
<thead>
<tr>
<th>Question</th>
<th>Answer</th>
</tr>
</thead>
<tbody>
<tr>
<td>A) Does the school have an IT Policy in place:</td>
<td>Yes ☑ No ☐</td>
</tr>
<tr>
<td>B) If possible can you copy the policy into the:</td>
<td>You will find it on our website.</td>
</tr>
<tr>
<td>Box:</td>
<td></td>
</tr>
<tr>
<td>-------------------------------------------------------------------</td>
<td></td>
</tr>
<tr>
<td>C) How are staff and pupils informed of the policy and any changes</td>
<td></td>
</tr>
<tr>
<td>in it?</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>Staff and pupils accept the policy the first time they log on the</td>
<td></td>
</tr>
<tr>
<td>computers each academic year, they cannot use the system until</td>
<td></td>
</tr>
<tr>
<td>they do this.</td>
<td></td>
</tr>
</tbody>
</table>

| D) Is IT training on best practices available to staff?          |
| - If possible please provide more information:                  |
|                                                                 |
| Yes  | No    |
|      | x     |

| E) Is training for staff on security and best practices for      |
| outside the organization available?                              |
|                                                                 |
| Yes  | No    |
|      | x     |

| F) Is IT training on best practices available to pupils?         |
| - If possible please provide more information:                  |
|                                                                 |
| Yes  | No    |
|      | x     |

| G) Is there any further information you would like to share that |
| can help me with my project please?                              |
|                                                                 |
| Happy to answer any follow up questions or get my network       |
| manager to do this same if it helps. We are currently having a   |
| massive network change and will be dealing with many security   |
| related issues.                                                 |

Thanks for taking part in the questionnaire. Your time and information is much appreciated.

Please sign the form at the bottom so I can use the data provided.

Kirk Kus – University of Derby

Email address: K.Kus1@unimail.derby.ac.uk
9.3. Questionnaires from school 3

KIRK KUS – UNIVERSITY OF DERBY – FINAL YEAR PROJECT QUESTIONNAIRE
20 January 2016

THE SECURITY EFFECTS OF BRING YOUR OWN DEVICE (BYOD) IN SCHOOLS:

Questionnaire for educational institutions that already have BYOD installed.

Information on the project: My final year project at the University of Derby is on the security implications of Bring Your Own Device for educational institutions. My research will help build a report on BYOD recommendations that schools should consider to protect the security of children’s information and prevent it from falling into the wrong hands. All responses will be kept in confidence, more details can be found on the consent documents that were attached to the questionnaire.

QUESTIONNAIRE.

1. Your details.
   A) Position: Network Manager
   B) Date: 01/03/2016

2. School information:
   A) School’s name: [Redacted]

3. BYOD information:
   A) Year when BYOD was implemented: 2012
   B) Who has access to the BYOD:
      - Pupils: X
      - Teachers: X
      - Associates: X
      - Guest: X
<table>
<thead>
<tr>
<th>C) What kind of access does each group have:</th>
<th>Full Network Access</th>
<th>Internet Only</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pupils:</td>
<td>☑️ Through RDP only</td>
<td>☑️</td>
</tr>
<tr>
<td>Teachers:</td>
<td>☑️ Through RDP only</td>
<td>☑️</td>
</tr>
<tr>
<td>Associates:</td>
<td>☑️</td>
<td></td>
</tr>
<tr>
<td>Guest:</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>D) Has the school ever had a security breach to its network via wireless or BYOD:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes:</td>
</tr>
<tr>
<td>No:</td>
</tr>
<tr>
<td>X</td>
</tr>
<tr>
<td>if No please go to question H)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>E) How many of these attacks has your organisation had via wireless:</th>
</tr>
</thead>
<tbody>
<tr>
<td>DoS attack</td>
</tr>
<tr>
<td>Authentication attack</td>
</tr>
<tr>
<td>Availability attack</td>
</tr>
<tr>
<td>Authentication attack</td>
</tr>
<tr>
<td>Man in the Middle attack</td>
</tr>
<tr>
<td>Eavesdropping</td>
</tr>
<tr>
<td>Other:</td>
</tr>
<tr>
<td>If other please state:</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>G) If possible please state how were these threats detected:</th>
</tr>
</thead>
<tbody>
<tr>
<td>N/A</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>H) If possible please state how the school dealt with these attacks:</th>
</tr>
</thead>
<tbody>
<tr>
<td>N/A</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>I) What type of wireless security does your organisation's network have:</th>
</tr>
</thead>
<tbody>
<tr>
<td>None: ☑️</td>
</tr>
<tr>
<td>WEP: ☑️</td>
</tr>
<tr>
<td>WPA:</td>
</tr>
<tr>
<td>WPA2: ☑️</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>J) How do users authenticate onto the network using their own device:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Open guest network with /32 subnet mask restrictions. Personal devices are not given the WPA2 password for the full network used by school-issued workstations.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>K) Have the system ever had any of the following security attacks:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Malware</td>
</tr>
<tr>
<td>Spyware</td>
</tr>
<tr>
<td>Worm: ☑️ &quot;Capshaw&quot;</td>
</tr>
<tr>
<td>Trojans</td>
</tr>
<tr>
<td>L) How were these threats detected:</td>
</tr>
<tr>
<td>M) How did the school deal with these attacks:</td>
</tr>
<tr>
<td>N) Approximately how many users connect to the wireless network using their own devices:</td>
</tr>
<tr>
<td>P) What kind of wireless attack detection system are in place within the network:</td>
</tr>
<tr>
<td>Q) Are different types of users on the wireless network on different VLANS:</td>
</tr>
<tr>
<td>R) Is VPN used for those who use their own device to access data from the school network:</td>
</tr>
<tr>
<td>S) What other security measures has the school taken to ensure that BYOD technology is secure:</td>
</tr>
<tr>
<td>T) Is there any other security information you would like to share for new organisations:</td>
</tr>
</tbody>
</table>
### 4. **Policy and training information:**

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>A) Does the school have an IT Policy in place?</td>
<td>Yes</td>
</tr>
<tr>
<td>B) If possible can you copy the policy into the box:</td>
<td>Too long — staff one attached to the e-mail instead. A similar one exists for students.</td>
</tr>
<tr>
<td>C) How are staff and pupils informed of the policy and any changes in it?</td>
<td>Unknown — I myself was not aware that the governors had reviewed it in January until today. It does not appear to have actually changed materially since I have been here.</td>
</tr>
<tr>
<td>D) Is IT training on best practices available to staff:</td>
<td>Yes</td>
</tr>
<tr>
<td>- If possible please provide more information:</td>
<td>But infrequent owing to lack of time on the CPD schedule</td>
</tr>
<tr>
<td>E) Is training for staff on security and best practices for using IT equipment outside the organization available:</td>
<td>Yes</td>
</tr>
<tr>
<td>- If only ad hoc and if requested</td>
<td>But only ad hoc and if requested</td>
</tr>
<tr>
<td>F) Is IT training on best practices available to pupils:</td>
<td>Yes</td>
</tr>
<tr>
<td>- If possible please provide more information:</td>
<td>But no statutory delivery exists</td>
</tr>
<tr>
<td>G) Is there any further information you would like to share that can help me with my project please:</td>
<td>I am happy to have a telephone/skype conversation to discuss anything I have mentioned — or any other related issues — in more detail to provide some background and an 'insider perspective' on how IT works within the education sector.</td>
</tr>
</tbody>
</table>

Thanks for taking part in the questionnaire. Your time and information is much appreciated.

Please sign the form at the bottom so I can use the data provided.

Kirk Kus — University of Derby
9.4. **Questionnaires from school 4**

---

**KIRK KUS – UNIVERSITY OF DERBY – FINAL YEAR PROJECT QUESTIONNAIRE**

20 January 2016

**THE SECURITY EFFECTS OF BRING YOUR OWN DEVICE (BYOD) IN SCHOOLS:**

Questionnaire for educational institutions that already have BYOD installed.

---

**QUESTIONNAIRE.**

1. **Your details.**

| A) Position: | ICT Manager |
| B) Date:     | 19 May 2016  |

2. **School information:**

| A) School’s name: | [Redacted] |

3. **BYOD information:**

| A) Year when BYOD was implemented: | 2015 (for staff and sixth form students only) |
| B) Who has access to the BYOD:    |  |
| Pupils (Sixth form)               | X |
| Teachers:                         | X |
| Associates:                       | X |
| Guest:                            | X |
### C) What kind of access does each group have:

<table>
<thead>
<tr>
<th></th>
<th>Full Network Access</th>
<th>Internet Only</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pupils</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Teachers</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Associates</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Guest</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### D) Has the school ever had a security breach via wireless or BYOD:

- [ ] Yes
- [x] No

If No please go to question H)

### F) How many of these attacks has your organisation had via wireless:

- [ ] DDoS attack
- [ ] Authentication attack
- [ ] Availability attack
- [ ] Authentication attack
- [ ] Man in the Middle attack
- [ ] Eavesdropping
- [ ] Other:
    - [ ] If other please state: 

### G) If possible please state how were these threats detected:

- [ ] 

### H) If possible please state how the school dealt with these attacks:

The only issue we've come across is some students sharing their username/ password to access the guest WiFi. Login account and device then disabled.

### I) What type of wireless security does your organisation's network have:

- [ ] None:
- [ ] WEP:
- [x] WPA2

### J) How do users authenticate onto the network using their own device:

- [ ] Ruckus via LDAP to Active Directory (username/ password)

### K) Have the system ever had any of the following security attacks:

- [ ] Malware
- [ ] Spyware
- [ ] Worm:
- [ ] Trojans
<table>
<thead>
<tr>
<th>Question</th>
<th>Response</th>
</tr>
</thead>
<tbody>
<tr>
<td>1) How were these threats detected?</td>
<td></td>
</tr>
<tr>
<td>2) How did the school deal with these attacks?</td>
<td></td>
</tr>
<tr>
<td>3) Approximately how many users connect to the wireless network using their own devices:</td>
<td>100-200 AVERAGE</td>
</tr>
<tr>
<td>4) What kind of wireless attack detection system is in place within the network?</td>
<td>Sophos UTM on the guest network, Ruckus controls the WIFI access.</td>
</tr>
<tr>
<td>5) Are different types of users on the wireless network on different VLANs?</td>
<td>Yes ✗ No</td>
</tr>
<tr>
<td>6) Is VPN used for those who use their own device to access data from the school network?</td>
<td>Yes ✗ No</td>
</tr>
<tr>
<td>7) What other security measures has the school taken to ensure that BYOD technology is secure?</td>
<td>Smoothwall manages the website filtering for staff and pupils. Sophos UTM firewall locks down the guest vlan network and monitoring software would detect network flooding. LAN Switches configured to detect and prevent broadcast storms and loops. Users cannot access guest WIFI unless they are in specific Active directory security groups.</td>
</tr>
<tr>
<td>8) Is there any other security information you would like to share for new organizations?</td>
<td></td>
</tr>
</tbody>
</table>

4. Policy and training information

<table>
<thead>
<tr>
<th>Question</th>
<th>Response</th>
</tr>
</thead>
<tbody>
<tr>
<td>9) Does the school have an IT Policy in place?</td>
<td>Yes ✗ No Acceptable Use Policy, Internet Policy, BYOD policy</td>
</tr>
<tr>
<td>Question</td>
<td>Answer</td>
</tr>
<tr>
<td>-------------------------------------------------------------------------</td>
<td>------------------------------------------------------------------------</td>
</tr>
<tr>
<td>B) If possible can you copy the policy into the box:</td>
<td>BYOD policy attached</td>
</tr>
<tr>
<td>C) How are staff and pupils informed of the policy and any changes in it:</td>
<td>The school policies are published to the school website and updated accordingly</td>
</tr>
<tr>
<td>D) Is IT training on best practices available to staff:</td>
<td>Yes, periodically during INSET training sessions</td>
</tr>
<tr>
<td>- If possible please provide more information:</td>
<td></td>
</tr>
<tr>
<td>E) Is training for staff on security and best practices for using IT equipment outside the organization available:</td>
<td>Not recently but any serious risks concerns are emailed.</td>
</tr>
<tr>
<td>F) Is IT training on best practices available to pupils:</td>
<td>Covered in the ICT lessons; specifically Internet Safety</td>
</tr>
<tr>
<td>- If possible please provide more information:</td>
<td></td>
</tr>
<tr>
<td>G) Is there any further information you would like to share that can help me with my project please:</td>
<td></td>
</tr>
</tbody>
</table>

Thanks for taking part in the questionnaire. Your time and information is much appreciated.

Please sign the form at the bottom so I can use the data provided.

Kirk Kus – University of Derby

Email address: K.Kus1@unimail.derby.ac.uk
9.5. **Questionnaires from school 5**

---

**KIRK KUS – UNIVERSITY OF DERBY – FINAL YEAR PROJECT QUESTIONNAIRE**

20 January 2016

**THE SECURITY EFFECTS OF BRING YOUR OWN DEVICE (BYOD) IN SCHOOLS:**

Questionnaire for educational institutions that already have BYOD installed.

---

**QUESTIONNAIRE.**

1. **Your details.**

   | A) Position: | IT Manager |
   | B) Date:     | 2 March 2016 |

2. **School information:**

<table>
<thead>
<tr>
<th>A) School's name:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
</tr>
</tbody>
</table>

3. **BYOD information:**

   | A) Year when BYOD was implemented: | September 2015 ready for start of new academic year (however, there has been an open policy for girls to bring their own devices, laptops, etc. for over ten years). |
   | B) Who has access to the BYOD:    |
   | Pupils: |   |
   | Teachers: |   |
   | Associates: |   |
   | Guest: |   |

---

1
<table>
<thead>
<tr>
<th>C) What kind of access does each group have:</th>
<th>Full Network Access</th>
<th>Internet Only</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pupils:</td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>Teachers:</td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>Associates:</td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>Guest:</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

D) Has the school ever had a security breach to its network via wireless or BYOD:
- Yes [ ]
- No [ ]
  If No please go to question H)

F) How many of these attacks has your organisation had via wireless:
- Denial of Service (DoS) attack [ ]
- Authentication attack [ ]
- Availability attack [ ]
- Authentication attack [ ]
- Man in the Middle attack [ ]
- Eavesdropping [ ]
- Other: [ ]
  If other please state: [ ]

G) If possible please state how were these threats detected:
- NA

H) If possible please state how the school dealt with these attacks:
- None: [ ]
- WEP: [ ]
- WPA: [ ]
- WPA2: [ ]

I) What type of wireless security does your organisation’s network have:
- Splash screen in browser that requires users AD username and password.

J) How do users authenticate onto the network using their own device:
- Malware: [ ]
- Spyware: [ ]
- Worm: [ ]
- Trojans: [ ]
### 3. Security and Environment

<table>
<thead>
<tr>
<th>Question</th>
<th>Response</th>
</tr>
</thead>
<tbody>
<tr>
<td>L) How were these threats detected?</td>
<td>N/A</td>
</tr>
<tr>
<td>M) How did the school deal with these attacks?</td>
<td>N/A</td>
</tr>
<tr>
<td>N) Approximately how many users connect to the wireless network using their own devices?</td>
<td>600 (this equates to around 1200 devices)</td>
</tr>
<tr>
<td>P) What kind of wireless attack detection system are in place within the network?</td>
<td>Inbuilt security in managed wireless solution. Firewalls and intranet filters in place.</td>
</tr>
<tr>
<td>Q) Are different types of users on the wireless network on different VLANs?</td>
<td>Yes (X) No ( )</td>
</tr>
<tr>
<td>R) Is VPN used for those who use their own device to access data from the school network?</td>
<td>Yes (X) No ( )</td>
</tr>
<tr>
<td>S) What other security measures has the school taken to ensure that BYOD technology is secure?</td>
<td>N/A</td>
</tr>
<tr>
<td>T) Is there any other security information you would like to share for new organisations?</td>
<td>N/A</td>
</tr>
</tbody>
</table>

### 4. Policy and Training Information

<table>
<thead>
<tr>
<th>Question</th>
<th>Response</th>
</tr>
</thead>
<tbody>
<tr>
<td>A) Does the school have an IT Policy in place?</td>
<td>Yes (X) No ( )</td>
</tr>
<tr>
<td>B) If possible can you copy the policy into the box:</td>
<td>Attached as separate documents.</td>
</tr>
</tbody>
</table>
C) How are staff and pupils informed of the policy and any changes in it?

<table>
<thead>
<tr>
<th>Question</th>
<th>Response</th>
</tr>
</thead>
<tbody>
<tr>
<td>All staff and students sign the policy when they join the school.</td>
<td></td>
</tr>
<tr>
<td>If changes are required then end-users are notified, though they are</td>
<td></td>
</tr>
<tr>
<td>not expected to re-sign the form.</td>
<td></td>
</tr>
<tr>
<td>D) Is IT training on best practices available to staff?</td>
<td></td>
</tr>
<tr>
<td>- If possible please provide more information:</td>
<td></td>
</tr>
<tr>
<td>Yes</td>
<td>x</td>
</tr>
<tr>
<td>No</td>
<td></td>
</tr>
<tr>
<td>Bespoke training available on demand and regular training sessions with</td>
<td></td>
</tr>
<tr>
<td>regard to IT held during INSET days.</td>
<td></td>
</tr>
<tr>
<td>E) Is training for staff on security and best practices for using IT</td>
<td></td>
</tr>
<tr>
<td>equipment outside the organization, available:</td>
<td></td>
</tr>
<tr>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>No</td>
<td>x</td>
</tr>
<tr>
<td>However, staff are briefed on best practice.</td>
<td></td>
</tr>
<tr>
<td>F) Is IT training on best practices available to pupils?</td>
<td></td>
</tr>
<tr>
<td>- If possible please provide more information:</td>
<td></td>
</tr>
<tr>
<td>Yes</td>
<td>x</td>
</tr>
<tr>
<td>No</td>
<td></td>
</tr>
<tr>
<td>This is covered in IT lessons and PSHE.</td>
<td></td>
</tr>
<tr>
<td>G) Is there any further information you would like to share that can</td>
<td></td>
</tr>
<tr>
<td>help me with my project please:</td>
<td></td>
</tr>
<tr>
<td>N/A</td>
<td></td>
</tr>
</tbody>
</table>

Thanks for taking part in the questionnaire. Your time and information is much appreciated.

Please sign the form at the bottom so I can use the data provided.

Kirk Kus – University of Derby

Email address: K.Kus@unimail.derby.ac.uk
9.6. **Questionnaires from school 6**

---

**KIRK KUS – UNIVERSITY OF DERBY – FINAL YEAR PROJECT QUESTIONNAIRE**

20 January 2016

---

**THE SECURITY EFFECTS OF BRING YOUR OWN DEVICE (BYOD) IN SCHOOLS:**

Questionnaire for educational institutions that already have BYOD installed

---

**1. **Information on the project:** My final year project at the University of Derby is on the security implications of Bring Your Own Device for educational institutions. My research will help build a report on BYOD recommendations that schools should consider to protect the security of children’s information and prevent it from falling into the wrong hands. All responses will be kept in confidence; more details can be found on the consent document that was attached to the questionnaire.

---

**2. QUESTIONNAIRE.**

1. **Your details:**

<table>
<thead>
<tr>
<th>A) Position:</th>
<th>IT Manager</th>
</tr>
</thead>
<tbody>
<tr>
<td>B) Date:</td>
<td>2 March 2016</td>
</tr>
</tbody>
</table>

---

2. **School information:**

<table>
<thead>
<tr>
<th>A) School’s name:</th>
</tr>
</thead>
</table>

---

3. **BYOD information:**

<table>
<thead>
<tr>
<th>A) Year when BYOD was implemented:</th>
<th>September 2015 ready for start of new academic year (however, there has been an open policy for girls to bring their own devices, laptops, etc., for over ten years).</th>
</tr>
</thead>
<tbody>
<tr>
<td>B) Who has access to the BYOD:</td>
<td></td>
</tr>
<tr>
<td>Pupils:</td>
<td>X</td>
</tr>
<tr>
<td>Teachers:</td>
<td>X</td>
</tr>
<tr>
<td>Associates:</td>
<td>X</td>
</tr>
<tr>
<td>Guest:</td>
<td>X</td>
</tr>
<tr>
<td>C) What kind of access does each group have:</td>
<td>Full Network Access</td>
</tr>
<tr>
<td>------------------------------------------</td>
<td>---------------------</td>
</tr>
<tr>
<td>Pupils:</td>
<td>x</td>
</tr>
<tr>
<td>Teachers:</td>
<td></td>
</tr>
<tr>
<td>Associates:</td>
<td>x</td>
</tr>
<tr>
<td>Guest:</td>
<td></td>
</tr>
</tbody>
</table>

| D) Has the school ever had a security breach to its network via wireless or BYOD: |
|-----------------------------------|-------------------|
| Yes                               |                   |
| No                                | x                 |
| if No please go to question H)    |                   |

<table>
<thead>
<tr>
<th>F) How many of these attacks has your organisation had via wireless:</th>
</tr>
</thead>
<tbody>
<tr>
<td>DoS attack</td>
</tr>
<tr>
<td>Authentication attack</td>
</tr>
<tr>
<td>Availability attack</td>
</tr>
<tr>
<td>Authentication attack</td>
</tr>
<tr>
<td>Man In the Middle attack</td>
</tr>
<tr>
<td>Eavesdropping</td>
</tr>
<tr>
<td>Other:</td>
</tr>
</tbody>
</table>

If other please state: 

<table>
<thead>
<tr>
<th>G) If possible please state how were these threats detected:</th>
</tr>
</thead>
<tbody>
<tr>
<td>NA</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>H) If possible please state how the school dealt with these attacks:</th>
</tr>
</thead>
<tbody>
<tr>
<td>NA</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>I) What type of wireless security does your organisation’s network have:</th>
</tr>
</thead>
<tbody>
<tr>
<td>None:</td>
</tr>
<tr>
<td>WEP:</td>
</tr>
<tr>
<td>WPA:</td>
</tr>
<tr>
<td>WPA2:</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>J) How do users authenticate onto the network using their own device:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Splash screen in browser that requires users AD username and password.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>K) Have the system ever had any of the following security attacks:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Malware</td>
</tr>
<tr>
<td>Spyware</td>
</tr>
<tr>
<td>Worm:</td>
</tr>
<tr>
<td>Trojans</td>
</tr>
</tbody>
</table>
**Virus**

**Other:**

*If other please state type:

<table>
<thead>
<tr>
<th>Question</th>
<th>Response</th>
</tr>
</thead>
<tbody>
<tr>
<td>L) How were these threats detected?</td>
<td>N/A</td>
</tr>
<tr>
<td>M) How did the school deal with these attacks?</td>
<td>N/A</td>
</tr>
<tr>
<td>N) Approximately how many users connect to the wireless network using their own devices:</td>
<td>600 (this equates to around 1200 devices)</td>
</tr>
<tr>
<td>P) What kind of wireless attack detection system are in place within the network:</td>
<td>Inbuilt security in managed wireless solution. Firewalls and intramet filters in place.</td>
</tr>
<tr>
<td>Q) Are different types of users on the wireless network on different VLANs:</td>
<td>Yes [x] No</td>
</tr>
<tr>
<td>R) Is VPN used for those who use their own device to access data from the school network:</td>
<td>Yes [x] No</td>
</tr>
<tr>
<td>S) What other security measures have the school taken to ensure that BYOD technology is secure:</td>
<td>N/A</td>
</tr>
<tr>
<td>T) Is there any other security information you would like to share for new organisations:</td>
<td>N/A</td>
</tr>
</tbody>
</table>

### 4. Policy and training information

<table>
<thead>
<tr>
<th>Question</th>
<th>Response</th>
</tr>
</thead>
<tbody>
<tr>
<td>A) Does the school have an IT Policy in place:</td>
<td>Yes [x] No</td>
</tr>
<tr>
<td>B) If possible can you copy the policy into the box:</td>
<td>Attached as separate documents.</td>
</tr>
<tr>
<td>C) How are staff and pupils informed of the policy and any changes in it:</td>
<td>All staff and students sign the policy when they join the school. If changes are required then end users are notified, though they are not expected to re-sign the form.</td>
</tr>
<tr>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td>D) Is IT training on best practices available to staff:</td>
<td>Yes ☑️ No ☐ Bespoke training available on demand and regular training sessions with regard to IT held during INSET days.</td>
</tr>
<tr>
<td>- If possible please provide more information:</td>
<td></td>
</tr>
<tr>
<td>E) Is training for staff on security and best practices for using IT equipment outside the organization, available:</td>
<td>Yes ☐ No ☑️ However, staff are briefed on best practice.</td>
</tr>
<tr>
<td>F) Is IT training on best practices available to pupils:</td>
<td>Yes ☑️ No ☐ This is covered in IT lessons and PSHCE.</td>
</tr>
<tr>
<td>- If possible please provide more information:</td>
<td></td>
</tr>
<tr>
<td>G) Is there any further information you would like to share that can help me with my project please:</td>
<td>N/A</td>
</tr>
</tbody>
</table>

Thanks for taking part in the questionnaire. Your time and information is much appreciated.

Please sign the form at the bottom so I can use the data provided.

Kirk Kuo – University of Derby

Email address: K.Kuo1@uninmail.derby.ac.uk
9.7. **Questionnaires from school 7**

**KIRK KUS – UNIVERSITY OF DERBY – FINAL YEAR PROJECT QUESTIONNAIRE**

20 January 2016

**THE SECURITY EFFECTS OF BRING YOUR OWN DEVICE (BYOD) IN SCHOOLS:**

Questionnaire for educational institutions that have **NOT** got BYOD installed.

Information on the project: My final year project at the University of Derby is on the security implications of Bring Your Own Device for educational institutions. My research will help build a report on BYOD recommendations that schools should consider to protect the security of children’s information and prevent it from falling into the wrong hands. All responses will be kept in confidence; more details can be found in the consent documents that were attached to the questionnaire.

**QUESTIONNAIRE.**

1. **Your details.**

   A) Position:  
   B) Date: 20/2/18

2. **School information.**

   A) School’s name: __________

3. **BYOD information.**

   A) Are you planning on installing BYOD in the near future:  
   - Yes [ ]
   - No [ ]
   - If Yes, please answer B) and move onto D)
   - If No, please go to question C)

   B) When are you planning to install BYOD in your organisation:  
   - Within a month: [ ]
   - 1 – 3 months’ time: [ ]
   - 3 – 6 months’ time: [ ]
   - 6 months’ – 1 year: [ ]
   - 1 – 2 years: [ ]
C) If A - Never, please can you give details why you are not planning to install BYOD: 

Principal’s policy of no mobile device it to be seen or used in school. This is to prevent bullying from those with big brand names to those with cheaper budget devices or nothing at all. There is also the issue of insurance.

D) Are there security issues with BYOD that are of concern to you: 

no

E) Does your organisation have a wireless system: 

Yes [ ]
No [ ]
If No please go to question J)

F) What type of wireless security does the organisation network have: 

None: [ ]
WEP: [ ]
WPA: [ ]
WPA2: [ ]

G) How many different devices connect to the wireless network on average in a day: 

500

H) Have you ever had an attack on your network, if so please give details: 

If no, please go to question J)

I) How was the attack dealt with: 

J) Are there any other security information you like to share for new organisations: 

Get your group policies correct

4. Policy and training information:

A) Does the school have an IT Policy in place: 

Yes [ ]
No [ ]

B) If possible can you copy the policy into the
<table>
<thead>
<tr>
<th>Box:</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>C) How are staff and pupils informed of the policy and any changes</td>
<td>They must accept at each login</td>
</tr>
<tr>
<td>in it?</td>
<td></td>
</tr>
<tr>
<td>D) Is IT training on best practices available to staff?</td>
<td>Yes [ ]</td>
</tr>
<tr>
<td>- If possible please provide more information.</td>
<td>No [ ]</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>E) Is training for staff on security and best practices for outside</td>
<td>Yes [ ]</td>
</tr>
<tr>
<td>the organization available?</td>
<td>No [ ]</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>F) Is IT training on best practices available to pupils?</td>
<td>Yes [ ]</td>
</tr>
<tr>
<td>- If possible please provide more information.</td>
<td>No [ ]</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>G) Is there any further information you would like to share that</td>
<td></td>
</tr>
<tr>
<td>can help me with my project please?</td>
<td></td>
</tr>
</tbody>
</table>

Thanks for taking part in the questionnaire. Your time and information is much appreciated.

Please sign the form at the bottom so I can use the data provided.

Kirk Kus – University of Derby

Email address: K.Kus1@unistail.derby.ac.uk
### Questionnaires from school 8

**KIRK KUS – UNIVERSITY OF DERBY – FINAL YEAR PROJECT QUESTIONNAIRE**

20 January 2016

**THE SECURITY EFFECTS OF BRING YOUR OWN DEVICE (BYOD) IN SCHOOLS:**

Questionnaire for educational institutions that have **NOT** got BYOD installed.

Information on the project: My final year project at the University of Derby is on the security implications of Bring Your Own Device for educational institutions. My research will help build a report on BYOD recommendations that schools should consider to protect the security of children’s information and prevent it from falling into the wrong hands. All responses will be kept in confidence, more details can be found on the consent documents that were attached to the questionnaire.

---

**QUESTIONNAIRE.**

1. **Your details:**
   
   | A) Position: | IT Technician (Level 2) |
   | B) Date:     | 12/04/2016              |

2. **School information:**
   
   | A) School’s name: | [Name Redacted] |

3. **BYOD information:**
   
   | A) Are you planning on installing BYOD in the near future: |
   | Yes ☐ No ☐ |
   | If Yes Please answer B) and move onto D) If No please go to question C) |

   | B) When are you planning to install BYOD in your organisation: |
   | Within a month: |
   | 1 – 3 months’ time: |
   | 3 – 6 months’ time: |
   | 6 months – 1 year: |
   | 1 – 2 years: |

1
C) If A – Never, please can you give details why you are not planning to install BYOD:

There are no plans at the moment. The issues are:
1. Bandwidth – the school can only afford a particular level of bandwidth 5% of which is allocated for ‘Guest’ devices. The other 95% is often used at full capacity and so if the percentage split were changed or the students were allowed to use the wifi networks on the 95% it would impact on the use of the bandwidth for teaching or the business of the school.
2. Behaviour management – the current school policy is that students must not bring mobile phones to school and if they need to then they are handed in until needed and must not be used in lessons. In actuality, well over 50% of students do bring their phones and keep them and teachers make a decision on a lesson by lesson basis about allowing use (mainly for listening to music). However this can be difficult to manage with some students using their phones when asked not to leading to disruption of learning. A recent observational visit of the school by advisors from the local authority also criticised the use of phones in lessons.
3. Those without devices – while most have a phone or tablet there are those who do not or do not have a smart phone. The reasons can vary from financial situations to parenting decisions. The school has a strict uniform policy to avoid bullying based on what students can afford to wear and encouraging the use of mobile devices could cause similar problems. The school has 10 iPads which could be lent to students without a device but that was not what they were intended for and 10 would probably not be enough. The school does not have the finances for more at the moment.

D) Are there security issues with BYOD that are of concern to you:

Some apps require the use of network login credentials which students will most likely happily provide but could then be used to attack the school network.

E) Does your organisation have a wireless system:

Yes [X]
No [ ]
If No please go to question J)

F) What type of wireless security does the organisation network have:

None [ ]
WEP [ ]
WPA [ ]
WPA2 [X]

G) How many different devices connect to the wireless network on average in a day:

100 devices

H) Have you ever had an attack on your network, if so please give details:

Not in the year I have been at the school but this is because of the security in place which BYOD could compromise.
4. Policy and training information:

<table>
<thead>
<tr>
<th>A) Does the school have an IT Policy in place?</th>
<th>Yes</th>
<th>No</th>
</tr>
</thead>
<tbody>
<tr>
<td>B) If possible can you copy the policy into the box?</td>
<td>It is many pages long – find attached to the email</td>
<td></td>
</tr>
<tr>
<td>C) How are staff and pupils informed of the policy and any changes in it?</td>
<td>Staff via email and students via assemblies, tutor time or Computing lessons</td>
<td></td>
</tr>
<tr>
<td>D) Is IT training on best practices available to staff?</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>- If possible please provide more information</td>
<td>Best practice is encouraged in the IT policy, by emails, at staff meetings and individually when working with staff</td>
<td></td>
</tr>
<tr>
<td>E) Is training for staff on security and best practices for outside the organization available?</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>- If possible please provide more information</td>
<td>See above</td>
<td></td>
</tr>
<tr>
<td>F) Is IT training on best practices available to pupils?</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>- If possible please provide more information</td>
<td>As part of Computing lessons which all students take in years 7, 8 and 9</td>
<td></td>
</tr>
<tr>
<td>G) Is there any further information you would like to share that can help me with my project please?</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Thanks for taking part in the questionnaire. Your time and information is much appreciated.

Please sign the form at the bottom so I can use the data provided.
9.9.  Policies document from school 3
ICT Acceptable Use
Policy and Practice

January 2016

Date Agreed by staff and governors: 11.01.16
Next review date: January 2017

“Achievement for All”
CONTENTS:

PURPOSE .........................................................................................................................2
SCOPE ............................................................................................................................2
USE OF EQUIPMENT AND MATERIALS .........................................................................3
  Use of Facilities ........................................................................................................3
  Facilities for Private Use ........................................................................................3
INADVERTENT ACCESS TO INAPPROPRIATE SITES AND
INAPPROPRIATE EMAILS .................................................................................................4
SCHOOL MONITORING ..................................................................................................5
ACCESS TO AND RETENTION OF MONITORING INFORMATION ..........................5
SURVEILLANCE ..............................................................................................................6
SECURITY ........................................................................................................................6
REPORTING MISUSE ......................................................................................................6
CONSEQUENCES OF BREACH: DISCIPLINARY ACTION .............................................7
STAFF LAPTOP LOAN CONDITIONS ............................................................................7
STAFF AGREEMENT TO POLICY FORM .......................................................................8

PURPOSE
The policy has been developed to advise employees if, when and under what conditions they
may use the school’s communications and information systems for personal reasons. It sets
standards to ensure that employees understand the position and do not inadvertently use
communications and information in inappropriate circumstances.

The School recognises employees’ rights to privacy but needs to balance this with the
requirement on the School (as a public service) to act appropriately, with probity, to
safeguard its business systems, and to be seen to be doing so.

In applying the policy, the School will act in accordance with the Human Rights Act 1998 and
other relevant legislation and will recognise the need of employees to maintain work/life
balance.

SCOPE
This policy covers all forms of communication, information retrieval (from any source), media
and equipment, used for official business and regardless of origin, ownership or place of use,
for example:
  • mail systems (internal and external)
  • internet and intranet (small, web access and video conferencing)
  • tablets and smartphones
  • telephones (hard wired and mobile)
  • pagers
  • fax equipment
  • computers – this covers ANY computer used for work purposes, whether at the place of
    work or elsewhere (see Laptops For Teachers)
  • photocopying, printing and reproduction equipment
• recording / playback equipment
• documents and publications (any type or format)

The policy applies to all employees (as a contractual term), agency staff and to other people acting in a similar capacity to an employee. It will also apply to staff of Contractors and other individuals providing services/support to the School (e.g. volunteers). It takes account of the requirements and expectations of all relevant legislation.

Headteachers will discuss the policy with their teams and agree parameters within which team members will act. This will take into account for example, whether or not there is a public phone in the building, whether or not employees are able to leave the premises during break periods, etc., and should be in writing. Every employee will have the policy explained to them at induction, and be given a copy for future reference. If at any stage employees require further clarification, they should speak to their Headteacher in the first instance.

Where an employee needs to discuss personal information with Occupational Health, Personnel or their Trade Union, they will be given privacy to do this.

Headteachers will agree with Trade Union representatives the arrangements for using School communication and information systems which will be provided in accordance with trade union facilities agreement and the ACAS Code of Practice.

USE OF EQUIPMENT AND MATERIALS

Use of Facilities
Staff must not carry out personal activities during working hours, nor mix private business with official duties. Official equipment and materials should not be used for general private purposes without prior permission from the Headteacher or an appropriate line manager. This will usually be in writing or may be covered by the parameters agreed by the Headteacher with the team.

Facilities for Private Use
If an employee needs to use a School phone (e.g. at their desk) for private purposes that are permissible within this policy, the call should be timed and the office given the details immediately to enable the cost to be charged to the employee. Payment is not required where employees need to phone to notify someone they have been delayed at work or in other emergencies.

In terms of using other equipment and materials, the decision to allow such use is at the Headteacher’s discretion. However the following are provided as examples to illustrate where it might be reasonable for permission to be given for reasonable use for private purposes, under the conditions shown and after getting prior approval, in writing if this is required. The Headteacher or a senior manager may veto private use at any time if they consider that circumstances justify this in general or particular cases, e.g. because of improper use or over-use. A charge may be made for materials if the values are significant.

• Social or recreational activities associated with school employment.
• Regular activity for a legitimate voluntary body or charity - but prior written approval from a Senior Manager must be obtained.
• Training or development associated with School employment.
• Occasional and brief essential family communications or other personal messages. In emergencies permission might need to be obtained retrospectively or again this may be covered by the general parameters agreed with the team.
If given permission, approved acceptable private use should normally take place in the employee’s own time but where this is not practicable or sensible, any disruption to the employee’s official work or that of colleagues must be minimal. Official work will always take precedence.

All uses, whether for private or official purposes, must observe:
- the law
- Financial Regulations and Codes of Practice on Financial Management
- Terms of employment, especially the Code of Conduct for Employees
- Communications & Information Technology (ICT) Code of Practice

It is not acceptable to use school equipment and materials or an employee’s own equipment/materials in the workplace in any of the following contexts:
- Illicit activity.
- Activities for private gain.
- Personal shopping.
- Excessive personal messages.
- Playing games.*
- Gambling.
- Political comment or any campaigning.
- Personal communications to the media.
- Use of words or visual images that are offensive, distasteful or sexually explicit.
- Insulting, offensive malicious or defamatory messages or behaviour.
- Harassment or bullying.
- Random searching of the web.
- Accessing sites which could be regarded as sexually explicit pornographic or otherwise distasteful or offensive.
- Using message encryption or anonymised web search, except where encryption is required for official School business purposes.
- Racist, sexist or other conduct or messages which contravene the Council’s employment diversity policies.
- Actions which could embarrass the School or bring it into disrepute.

* except those games pre-loaded as part of the Microsoft programme suite, which may be accessed in the employee’s own time.

**INADVERTENT ACCESS TO INAPPROPRIATE SITES AND INAPPROPRIATE EMAILS**

If an employee inadvertently accesses an inappropriate web site, they should leave it immediately but notify the Headteacher/Senior Manager of the incident, giving the date and time, web address (or general description) of site and the action taken. This will help safeguard their position in circumstances where disciplinary action would otherwise result.

Employees may find themselves receiving emails which contravene this policy. In the case of comparatively innocuous material (e.g. ‘clean jokes’), the recipient should point out to the sender that they do not wish to receive such messages at their workplace because they believe they contravene the school’s/Council’s policy. If there is repetition, the employee should retain the messages and notify their Headteacher/Manager. If the emails are racist or sexist or could otherwise be regarded as offensive, they should be left in the inbox and the Headteacher/Manager notified immediately. Employees should notify the sender that they do not wish to receive further such material and keep a record of doing so.
SCHOOL MONITORING

Monitoring information will not be accessible (or distributed) any more widely than is necessary for the purposes for which it is needed.

All employees should be made aware at induction, at intervals thereafter and possibly through automatic messages on school equipment, that, in relation to any electronic communication, there can be no expectation of absolute privacy when using school/County equipment provided for official/ work purposes; and that the school reserves the right to monitor all communications including their content. This monitoring is carried out to ensure that equipment and systems are used efficiently and effectively, to maintain systems security and to detect any breaches of this policy or the law. Normally monitoring consists of the following:

- **Telephones and fax.** The School reserves the right to monitor communication content selectively if abuse is suggested. However such monitoring would only take place following an assessment that such steps are necessary to further a particular investigation or concern. It would only be authorised following the advice of the Council’s Statutory Officers. Where calls are made via the CCC network, an automatic record is kept of every number called, from where and the duration of the call. Further action is taken where particular numbers called or the frequency and duration of calls suggest abuse of this policy. Telephone response times will be sampled from time to time.

- **Emails.** When using the Cheshire East County Council network, every incoming and outgoing email message is automatically swept for key words which could indicate misuse. The school reserves the right to apply similar screening to its own email systems.

- **Web access.** When using the Cheshire East County Council network, access to some web sites is automatically prevented (e.g. pornographic, racist and violent sites) and others are restricted (e.g. MP3 music sites and Web Chat) and a message warns that these types of sites are strictly for business purposes. However, an automatic record is made of all sites visited and a sweep made of site names and content against pre-determined criteria, to identify inappropriate sites together with attempts made to access such sites. The school reserves the right to apply similar restrictions and screening to its own web access systems.

- **Mail.** The privacy of internal and external postal communications marked 'personal' will normally be respected (unless abuse of this policy is suspected) but all other communications may be opened for good reason by a Headteacher, manager, secretary or colleague.

ACCESS TO AND RETENTION OF MONITORING INFORMATION

In the case of Cheshire East County Council systems, access to routine monitoring information is restricted to specified employees in Information & Communication Technology Services and Audit. If they identify a potential issue of abuse the relevant Headteacher/Senior Manager will be given access to the information to enable appropriate action to be taken. They will respect the confidentiality of all communications and disclose the contents of communications only where there are grounds for suspecting abuse of this policy. Where this is the case, other Senior Managers may then be involved and are likely to be made aware of the contents of communications. This information would be held by the Headteacher, accessible by the Headteacher and if appropriate other Senior Staff, Governors.
SURVEILLANCE

Permanently fitted CCTV cameras are installed by the School, in the internal exclusion room, on the corridor by room 5 and in the central library area, for security and safety reasons and will always be visible to people within their range. Video recording, onto the computer server, will be kept secure, the information used only for security purposes. No automatic connections will be made between information from security cameras and other monitoring sources. CCTV cameras also cover areas around the sports hall and dining room, these are owned and managed by Congleton Borough Council.

CCTV monitoring will only be used in connection with a criminal investigation or where abuse of terms of employment, e.g. the sickness scheme, is being investigated. This will always be in accordance with the statutory safeguards applicable to such activity (the Regulation of Investigatory Powers Act and the Human Rights Act) and only authorised following careful consideration of the need for such action in accordance with the attached policy entitled "Surveillance under the Regulation of Investigatory Powers Act 2000".

This policy provides safeguards in relation to who can sanction covert surveillance (only the Monitoring Officer (County Solicitor) or his authorised deputy), the reasons it can be undertaken and how long it can continue.

SECURITY

Every employee must observe the school's/Council's communications and information technology security requirements (as detailed in the ICT Code of Practice) and act responsibly when using equipment and materials. Employees will be provided with the necessary briefing and training to enable them to comply with this requirement. The Headteacher will take the most serious view of any action or inaction on the part of an employee who deliberately, recklessly or carelessly jeopardises the security of records or systems. Any employee detecting a potential security problem (e.g. a virus or unauthorised access) must immediately take any action within their authorised power to safeguard or resolve the situation (e.g. disconnect any infected machine from the network (remove the cable) and, if appropriate, notify the person responsible for ICT) and notify the Headteacher or a senior manager.

REPORTING MISUSE

If any employee suspects activity which may constitute misuse or activities which could jeopardise system security, they must report this immediately to the Headteacher or a senior manager. The Headteacher or senior manager must consider whether it would be appropriate to involve Internal Audit and must always ensure that all relevant records and documents (paper and electronic) are safeguarded and retained securely. If necessary, a strategy for investigation will be agreed between the Headteacher/manager, Internal Audit and Schools' HR Consultancy, taking legal advice as necessary.

CONSEQUENCES OF BREACH: DISCIPLINARY ACTION

Breaches of this policy may result in the application of the Disciplinary Procedure and may, if deemed sufficiently serious, be treated as gross misconduct. In the case of Contractors, agency staff, volunteers or partnership employees, breach may result in termination of the contract or relevant arrangement and/or withdrawal of the relevant facility. Police involvement and prosecution may follow if the conduct in question constitutes possible criminal activity.
STAFF LAPTOP LOAN CONDITIONS

A laptop computer will be loaned to you while you remain employed by [School]. While the laptop is in your care the following items should be noted:

1. The Laptop remains the property of [School]. The laptop is for use in connection with MHS business only.

2. All laptops are issued to a nominated member of staff, it is this member of staff who is responsible for making sure that the laptop is kept secure at all times.

3. MHS Insurance cover provides protection from standard risks but excludes theft from an un-attended car.

4. Due to the increasing number of viruses that take advantage of operating system attacks Anti Virus and Windows Update must be carried out at a regularly. This is automatic when connected to the MHS network. It is the nominated member of staff’s responsibility to make sure the laptop’s security is up to date.

5. Should any faults occur the school’s IT support staff must be advised as soon as possible so that they may undertake any necessary repairs. Under no circumstances should staff attempt to fix suspected hardware faults.

6. Any charges incurred by using this laptop outside business use are not chargeable to the school. These charges will be the responsibility of the nominated member of staff.

7. Upon temporary or permanent loss of the laptop, the police should be notified immediately. The IT network manager should be informed as soon as is practical with a report of the circumstances, police incident number and a list of all business data lost, specifically detailing confidential data secure or unsecure (normal logon password is classed as unsecure).

8. Software licensed by the school, authorised by the Headteacher, or Network Manager on his behalf, and installed by the school’s IT support staff is the only software that the school takes legal responsibility for. Installed software will be checked during regular routine maintenance carried out by IT support staff and any irregularities reported to the network manager who may forward this information to the Headteacher or LA. Any software that is installed on the laptop that is not installed by IT Support is the legal responsibility of the nominated member of staff that the laptop belongs to, and not that of the school.
Name: _______________________________________

I have received and read a copy of the School Communications and Information Acceptable Use Policy and agree to abide by the procedures and guidance contained within it.

Signed  _______________________________________

Date  _______________________________________

Please complete the following information:

Laptop Make  _______________________________________

Model  _______________________________________

Serial Number  _______________________________________

Service Tag No.  _______________________________________

Date Issued  _______________________________________

BRING YOUR OWN DEVICE (BYOD) POLICY

The Academy recognises that as mobile technology has changed more pupils have access to Internet capable devices. For Sixth Formers this should be seen as a resource and provide an opportunity to enable quick and easy access to the Internet to enhance classroom learning.

General Information

Personal wireless device access is restricted to Internet only. Sixth Formers will not have access to any documents which reside on the Academy network. Internet traffic will be filtered through Smoothwall in the same way as Academy local area network Internet traffic.

Access to the guest wireless network is a privilege, not a right. Any use of the wireless network entails personal responsibility and compliance with all Academy rules. The use of the network also allows ICT helpdesk staff to conduct investigations regarding inappropriate Internet use at any time, via a teacher request.

Accessing the wireless network

Search for wireless networks and select ‘Magpie’. You will then be prompted to enter your username and password, which is the same username/password you enter to access the schools network.

Guidelines for Use

- Use of personal devices by sixth formers during the taught time and tutor time is at the discretion of teachers and staff. Sixth formers must use devices as directed by their teacher.

- The primary purpose of the use of personal devices at school is educational. Using the device for personal reasons e.g. contacting parents, should only take place outside of taught time and tutor time, and discretely. This means away from where pupils in Year 7-11 can see.

- The use of a personal device is not to be a distraction in any way to teachers or pupils. Personal devices must not disrupt class in any way.

- The use of personal devices falls within the Pupil (AUP) Acceptable Use Policy, found on our website.

- Sixth formers shall make no attempts to circumvent the Academy’s network security and/or filtering policies. This includes setting up proxies and downloading programs to bypass security.
• Sixth formers shall not distribute pictures or video of pupils or staff without their permission (distribution can be as small as emailing/texting to one other person or as large as posting image or video online).

Consequences for Misuse or Disruption
(some may apply)

• Access to the wireless network will be removed.
• Device taken away for the lesson.
• Device taken away and kept in the school office until the end of the school day for the first offence. The device may be kept for longer for repeat offences in line with procedures for lower school pupils, or at the discretion of the leadership team.
• Pupil is not allowed to use personal devices at Academy.

Serious misuse of Internet capable devices is regarded as a serious offence within the Academy’s Behaviour Management Policy and will be dealt with in accordance with this policy.

Academy Liability Statement

Sixth formers bring their devices to use at their own risk. Sixth formers are expected to act responsibly with regards to their own device, keeping it up to date and as secure as possible. It is their duty to be responsible for the upkeep and protection of their devices.

[Redacted] is in no way responsible for:

• Personal devices that are broken while at Academy or during Academy-sponsored activities
• Personal devices that are lost or stolen at Academy or during Academy-sponsored activities
• Maintenance or upkeep of any device (keeping it charged, installing updates or upgrades, fixing any software or hardware issues).

12 November 2015
9.11. **IT Policy for Staff - April 2015 from school 5**

**IT Policy for Staff**

School computers and data are exposed to a number of threats which can jeopardise the confidentiality, integrity and availability of our work. These include physical theft, identity theft, theft of confidential or sensitive information, and exposure to computer viruses or malware.

Further, a computer running on our network operates under conditions which differ from those at home. Threats may not only affect your work, which may be lost or corrupted, but also have serious consequences for the School.

- In mishandling personal data related to staff, students or parents, you and the School may be in breach of data protection laws, which may result in fines and significant reputation damage for the School.
- Viruses which spread across the network require lengthy work which may affect network performance and result in internet connections being blocked.
- Inappropriate use of a shared internet connection can lead to significant slowdown and loss of service.

The Policy on Authorised and Unauthorised Usage gives direction for using IT securely so that you put neither yourself nor the School at risk.

It should be read in tandem with the Responsible User Guide. This has specific sections on the following:

- Passwords
- E-mail
- Social networking
- Data security
- Laptop security and usage off site
- Tablets issued to staff by the school
- Own devices
- Remote working
- Annex A: E-mail protocol
- Annex B: Guidelines for classroom management of tablets and mobile devices
- Annex C: Social Media guidelines

**Policy on Authorised and Unauthorised Usage**

1. **Provides internet access and e-mail facilities to staff to facilitate**

- Research, teaching and learning
- Professional communication
- School administration
- Professional training
2. The following uses of the Internet and e-mail facilities are not authorised (although this list is not exhaustive):

- Chain mail and spam mail ("Spamming" is a term used to describe indiscriminate blitzing of e-mail messages to an entire community)
- Gambling
- Downloading programmes except when authorised by IT personnel
- Viewing, transmitting or downloading indecent content
- Private business interests
- Use of portal or proxy sites that bypass filtering
- Downloading of sensitive information from School databases onto laptop hard disks or unencrypted removable media;
- Uploading sensitive information to cloud storage such as Sky Drive or Dropbox

3. The School has no objection to members of staff using the Internet and e-mail facilities for private and/or personal purposes provided that:

- The purposes are not unauthorised
- Private and/or personal usage is appropriately proportional to professional activity
- Users accept that traffic is monitored to distinguish between use for authorised and unauthorised purposes
- Users accept that traffic is filtered to prevent use for unauthorised purposes

4. Accessing or downloading material for unauthorised purposes will constitute a disciplinary matter and it is the School's policy that any individual who accesses or downloads material of a pornographic, obscene, illegal, offensive or otherwise corrupt or depraved nature, will be guilty of gross misconduct for which the School is entitled to dismiss without notice.

The possession or sending of pornographic messages, images, bad language, offensive jokes or unwarranted advances will be treated as a disciplinary matter. You should take particular care in dealing with material that is sent to you and if you believe that any such material may place you in breach of this policy you should delete it from your work area and notify IT personnel.

5. To avoid importing any viruses, you must ensure that any files containing software which are downloaded from the Internet, are forwarded unopened to IT personnel.

If you are in any doubt as to the correct course of action, in relation to any proposed Internet or e-mail use, you should not act without seeking further advice from ICT personnel.

Reviewed April 2015

FC

IT Responsible User Guide

Passwords

Users are allocated a unique identifier (user ID) for their personal and sole use. Strong passwords are required for the School network. (A strong password is at least nine characters long, does not contain your user name or a complete dictionary word, is significantly different from previous passwords and contains characters from each of the following: upper case, lower case, numerals and symbols.)

All employees should take appropriate steps to safeguard them at all times.

Your password should not be shared. If you share your password with a colleague or friend, you may be held responsible for their actions.

Passwords should be changed annually or immediately if they may have been compromised.

E-mail

The e-mail system is predominantly for the purpose of the School’s communications and all e-mail messages and attachments (including private and personal e-mails and attachments) are records that are School property. The School has the right to intercept, monitor and review all e-mails and attachments that are at any time on or within the School’s e-mail system.

You should not assume that all e-mail is private or personal and it should be borne in mind that apparently deleted e-mail may exist on the system for some time and be accessible from backup files.

The School provides a protocol for the use of e-mail and all members of staff are expected to observe its terms. Any breach of this protocol may be treated as a disciplinary matter. The protocol is outlined at Annex A.

Social Networking and Video Sharing websites

The use of social networking sites within the School is allowed as permitted by our internet content filter (Total Traffic Control).

Examples of social networking sites include blogs, wikis, Facebook, Twitter, Pinterest, Windows Live Spaces, forums, bulletin boards, chatrooms and instant messenger.

The School expects every employee to have due regard for its good reputation. When logging on to and using social networking and video sharing websites and blogs at any time, including personal use on non-School computers outside the workplace, employees are advised that they should not

- publicly identify themselves as working for the School or make reference to the School
- use their work e-mail address when registering on such sites or provide any link to the School's website.
- communicate with students over social networking sites using their personal systems and equipment. Unwanted communications should be blocked.
- mix personal and professional accounts. Professional accounts must be used when teaching students the appropriate use of social networking sites.
- communicate with leavers of less than 2 years' standing using social networking and should be circumspect in communication with any leaver who may still have current friends within the School.
- include personal information or data about the School's employees, students, contractors, suppliers, parents or clients without their express consent (an employee may still be liable even if the School, its employees, students, contractors, suppliers, parents or clients are not expressly named in the websites or blogs as long as the School reasonably believes they are identifiable) - this could constitute a breach of the Data Protection Act 1998 which is a criminal offence.
- make any derogatory, offensive, discriminatory or defamatory comments or images about the School, its employees, students, contractors, suppliers, parents or clients (an employee may still be liable even if the School, its employees, students, contractors, suppliers, parents or clients are not expressly named in the websites or blogs as long as the School reasonably believes they are identifiable).
- make any comments about the School's employees or students that could constitute unlawful discrimination, harassment or bullying contrary to the Equality Act 2010 - you can be personally liable for your actions under the legislation.
- disclose any trade secrets or confidential or sensitive information belonging to the School, its employees, students, contractors, suppliers, parents or clients or any information which could be used by one or more of the School's competitors, for example information about the School's work, its products and services, technical developments and staff morale.
- breach copyright or any other proprietary interest belonging to the School.

Employees should remember that social networking websites are a public forum, even if they have set their account settings at a restricted access or “friends only” level, and therefore they should not assume that their entries on any website will remain private.

Employees must also be security conscious when using social networking websites and should take appropriate steps to protect themselves from identity theft, for example by restricting the amount of personal information they give out, such as date and place of birth, Schools attended, family names and favourite football team. This information may currently form the basis of security questions and/or passwords on other websites, such as online banking.

If employees are asked to contribute to an official blog or newsfeed connected to the School, then special rules apply and the employee will be briefed in detail about what to write.

The School provides a protocol for the use of social media and all members of staff are expected to observe its terms. Any breach of this protocol may be treated as a disciplinary matter. The protocol is outlined at Annex C.

**Data Security**

The School has a Data Protection Policy (see Policies) and provides training in Data Protection. The School’s Data Protection Officer is the Bursar. If you become aware of a breach of security, or have any concerns, you should inform the DPO.
You are responsible and liable for the data you handle.

Sensitive data includes personal data, commercial data, and any confidential matter not in the public domain.

- Wherever possible, work with the data on the School servers and entirely avoid the transfer of data onto laptop or any other device. This can be achieved by using the remote link to SAMS [REDACTED] or [REDACTED] in the case of [REDACTED].
- Please log off rather than leave a computer unattended in a classroom or other public area.

Laptop security and usage of removable media

Users of School laptops should take particular precautions when School laptops leave the premises. Users should understand that the greatest risk concerns any School data that may be present on the laptop which relates to individuals. The loss of such data through theft or abandonment presents a far greater hazard than the loss of the physical laptop owing to the breaches of the Data Protection Act that would occur. Other documents which do not relate to individuals have the capacity to damage the standing of the School as a result of misinterpretation or partial understanding of the context and objectives.

- Where it is essential (for example while travelling) to hold data on an offsite School laptop, the data should always be held on a temporary basis to be removed once the task in hand is completed. Holding data on an encrypted memory stick in place of the laptop can improve security in areas where a laptop might be vulnerable to theft in crowded terminals or thoroughfares. In this case the encrypted memory stick should be kept in a pocket or accessory and not in the laptop bag.
- Where data is particularly sensitive and the laptop is often taken offsite it should be considered that the routine deletion of files is not sufficient security against theft or loss, as the data is recoverable using a wide variety of technical processes. In these cases sensitive data should be held in a single folder, and the laptop should be brought to the IT department for cleansing when a significant task has been concluded.
- Users with laptops that have the bio password facility, normally a fingerprint, should use this added layer of security.
- Bluetooth – the Bluetooth protocol is used from time to time to link mobile devices to laptops. If you are familiar with this process or intend to use it, the devices must be paired and access granted through pin codes. An unsecured Bluetooth connection is potentially visible, for example, to all other laptop users in a railway carriage.

Passwording documents and laptops offers some protection against the casual hacker or opportunist thief but presents no real defence against professional IT resources. The same applies to low level encryption while high level encryption is overtly complex for School use. These additional measures can be used with prudence where the casual threat is high. For advice on their use please consult the IT department.
**Tablets issued to Staff by the school**

A separate user agreement must be signed prior to issue of the device.

These are managed via the School’s Mobile Device Management system. Apps may be purchased and installed via the IT support department. Apps are ordinarily to be purchased by departments. But the Deputy Head (Teaching and Learning) holds a small budget for generic apps.
If a device is owned by school, all data is owned by school.

Unlike the pupils, staff may take a school iPad off site, but may not lend the device to a third party.

Family and friends must not be invited to access school materials which may include pupils’ personal data (photographs are a case in point), so passwords must not be shared with them.

If the device is lost or stolen, staff should notify school immediately so that login details can be changed.

Report any problems to the IT department (there is a ticketing system on the VLE)

In addition:
- It is an expectation that all who have borrowed a device will contribute to any relevant evaluation exercise.
- Participants must familiarise themselves with current pupil ‘Ground rules and User agreement’.
- Unlike the pupils, staff may take the iPad off site, but may not lend the device to a third party.

**Practical points**
- Only use the device allocated to you.
- Only use the protective cover supplied by the school.
- Take care not to drop the device, to lose or damage it.
- Participants should be very circumspect about potential breach of data protection guidelines.
- In case of loss, report this immediately. Data may need to be remotely wiped.
- Be aware that personal material stored on the device, including photographs, is likely to be wiped when the iPad is handed back.
- You should be able to download free apps to your device. Other purchases should be made through the IT department.
- Guidelines for Classroom management of mobile devices are to be found in Annex B

**Own Devices**

Teachers and administrators may arrange to have their devices connected to the School network by the IT Support staff:

- The principles of protecting School data as outlined above apply.
- Where friends and family have access to a tablet owned by the individual teacher, no pupil data should be stored on the device. This includes photographs and work.
Ephemeral data should be erased, and other material must be transferred to school storage.

- If such a device is lost, stolen, or replaced, IT Support must be notified immediately so that the connection to SG can be severed.
- In order to acquire an app for use with pupils, the member of staff should contact the IT Support department who will be able to purchase and install under the "Managed Distribution" option. From September 2015, this is chargeable to departments.
- Before undertaking an activity, you are strongly advised to refer to the checklist pro forma on the VLE.
- Before you photograph or film other people, make sure you have their consent and move any such media to School owned storage as soon as is possible.
- Password protect any device so that if lost or stolen it is not instantly accessible.

Remote Working

Remote working is provided to members of staff by the School so that professional activities may be pursued at home at appropriate times.

- Under the terms of the Data Protection Act 1998 professional data in use at home (as with all such data) must not be disclosed to third parties and suitable vigilance must be applied within the home or mobile workplace to ensure that data is not compromised.

Reviewed April 2015
FC
Annex A

E-mail protocol

These guidelines have been prepared as part of the School’s ongoing commitment to improving the effectiveness of communication and the quality of working relationships within the community.
E-mail is a powerful tool but it is effective only for certain types of communication. Face to face or voice contact is frequently superior. For reasons of business clarity and to maintain professional relations the following protocol should be adhered to by all of those working at

Beneficial uses of e-mail

a) Appointments and meeting invitations (Outlook Calendar)
b) Routine announcements
c) Reminder or confirmation of previously agreed courses of action
d) Academic or pastoral care notifications
e) Following up issues on the horizon
f) Commercial correspondence
g) Agendas and Minutes

Usage to be avoided

a) Conveying news which will be surprising or unwelcome to the recipient(s)
b) Expressing negative emotions or criticism
c) Escalating issues
d) Conveying matters which are sensitive or highly confidential
e) Bulk mailing including non-School promotions
f) Document transfer where more economical and efficient means (eg a hyperlink to VLE page or other location) are available

Guidance on e-mail style and functionality

a) E-mails should be friendly or business-like in composition
b) The iSAMS e-mail client (say ‘Ag to Outlook when asked’) may be used if it is necessary to keep a structural record of the correspondence.
c) E-mails should be addressed to those from whom a predicted action is expected within a practical timescale.
d) E-mails should be copied sparingly, for information. If you are copied in to an e-mail there is no obligation to respond.
e) Replies to e-mails are not obligatory, in many straightforward instances replies may be waived.
f) E-mails are normally forwarded in cases of mistaken address or area of responsibility. Great care should be taken when forwarding in any other circumstances.
g) Group mail/distribution lists private to the sender are the first means of widening the pool of recipients.
h) Public list mails should be used only when there is a clear requirement to disseminate information widely.

i) E-mails regarding School matters or personnel are business records. As business records they are retained as fact and/or opinion of a business nature. They may subsequently be required or produced for evidential purposes.

Remember there is a person on the receiving end of every e-mail; in each instance recipients should have confidence that the guidance, direction, or information being sent is both constructive and helpful.
Annex B

Guidelines for Classroom management of tablets and mobile devices

- Ask girls to keep the tablet closed on the desk / out of the way when not in use.
- Clear identification of the parts of the lesson where they may, and may not, use the device is essential with 4th and 5th forms.
- Do be aware that if a girl has 3G on her own tablet she can easily go off-piste! So keep mobile - do walk around the class.
- Ensure there is no recording of any type – photography, film or audio - without the permission of those being recorded. In the context of a lesson, the device should only be used this way if you specifically suggest it.
- Do not base your lesson around something the girls may not have.
- The device is a great way of giving quick access to the internet.
- It can be helpful for girls with special needs to photograph the whiteboard or use the tablet to make notes.
- Before you encourage a girl to produce a piece of work for anyone other than herself, ensure you have a technical strategy for taking the work in or sharing it. Be mindful of your time and effort. (This is not a problem with ephemeral material, which can be trashed.)
Annex C

Social Media Guidelines

Social media is used extensively as a channel of communication. We believe that the instant nature of this medium, coupled with the possibility of two-way communication makes it a powerful tool and enhances our ability to keep in touch with our constituents. We value the flexibility that social media offers, and feel that it forms a vital part of our multi-channel approach to marketing. We are aware of the need to maintain our online presence in all the environments where our stakeholders converse and hence Facebook and Twitter are our social media tools of choice.

1. Introduction

The principles set out in these guidelines are designed to ensure that the use of social media among [redacted] is undertaken responsibly and that the confidentiality of students and staff, and the reputation of the school, are safeguarded.

2. Scope

These guidelines apply to [redacted] staff, parents and the wider school community. They cover personal use of social media, as well as the use of social media for official school purposes, including sites hosted and maintained on behalf of the school.

These guidelines apply to personal web space such as social networking sites (for example Facebook, Instagram, SnapChat), blogs, microblogs such as Twitter, chatrooms, forums, podcasts, open access online encyclopaedias such as Wikipedia, social bookmarking sites such as del.icio.us and content sharing sites such as flickr and YouTube.

Since it is impossible to cover all circumstances or emerging media, the principles set out in these guidelines should be followed irrespective of the medium.

3. Related policies

These guidelines should be read in conjunction with the following school policies:
- Code of conduct policies
- ICT policies for staff and students
- IT user policies
- Safeguarding policies
- Terms of agreement

All of these policies can be found on the school YLE.

4. Guidelines for students

4.1 Your online behaviour should reflect the same standards of honesty, respect and consideration that you use face-to-face
4.2 Your use of social media should be age appropriate e.g. only over 13s should be using Facebook
4.3 When posting comments or photos on social media channels, ask yourself whether you would be happy for your parents or your future employer to read your posts
4.4 Provide as little information about yourself as possible; not providing your date of birth or location will improve your online security
4.5 You should set your privacy settings on Facebook to Friends Only, but be aware that unless your friends’ settings are the same as yours, your posts may be seen more widely.

4.6 Think carefully before engaging with strangers in ‘open’ environments, especially Twitter; be aware that ‘protecting’ your tweets will improve your online security.

4.7 Do not attempt to ‘friend’ or follow staff on social media sites.

4.8 Do not tag or identify yourself (or other students) on Sherborne Girls social media sites; even when using your own accounts, you should ask permission before tagging someone in a photo.

4.9 Do not engage in any activities involving social media which might bring ______ into disrepute.

4.10 Do not engage in any abusive, threatening, unkind or bullying behaviour.

4.11 Use of profanity or threatening language is not acceptable.

4.12 Under no circumstances should negative comments be made about staff, parents or other students on social media sites.

4.13 _______ reserves the right to monitor social media activity and if students are found contravening the guidelines, then school sanctions will be imposed.

5. Guidelines for staff

5.1 You should decline ‘friend’ requests and/or block followers from students you receive in your personal social media accounts.

5.2 You should not accept any contact from a former student of the school if under the age of 18.

5.3 You should not have contact with a student’s family members through personal social media if that contact is likely to constitute a conflict of interest.

5.4 Don’t take photos or video with your own phone or camera – the Marketing team has equipment available for this.

5.5 If posting a photograph on an approved school social media platform, do not use the student’s full name if they are in the photo. You may only use their full name if no photo is used, or if the post is referencing something that has already been published about the student and is well-known e.g. a notable prize-winner.

5.6 Do not tag photographs of staff or students.

5.7 When using a hyperlink in any social media, check that the content is appropriate, especially if you are sharing it.

5.8 Don’t discuss personal information about other pupils, _______ and the wider community you interact with on any social media.

5.9 You should set your privacy settings on Facebook to Friends Only, but be aware that unless your friends’ settings are the same as yours, your posts may be seen more widely.

5.10 Passwords and other login information must be kept safely; remember to lock your work station when you leave it unattended.

5.11 School email addresses should not be used for setting up personal social media accounts or to communicate through such media.

5.12 All email communication between staff and members of the school community should be made from official school email accounts.

5.13 Don’t engage in activities involving social media which might bring _______ into disrepute.

5.14 If you are aware of any inappropriate communications involving any student in social media situation, please report it to the Deputy Head Pastoral.

5.15 If in any doubt regarding issues relating to specific students, please check with the Marketing team.
6. Guidelines for parents

6.1 The school will monitor, and where appropriate, moderate, content and activity on social media platforms.

6.2 The school cannot be held responsible for improper use of social media by students.

6.3 It is the responsibility of parents/guardians to monitor their daughter's activity on social media.

6.4 If you do not wish your daughter's name or photograph to be used in connection with the school's official social media platforms, website or PR, you will need to opt out when completing the New Girls information pack.

7. Using social media for marketing

The Marketing team runs the school's official website, Facebook, Twitter, YouTube and LinkedIn sites. A limited number of other staff (eg Sports, Old Girls) have administrator rights to post onto these sites. If you have any concerns about content you have viewed on school social media sites, you should contact marketin@guesthostname.

While pupils and the wider school community are encouraged to interact with these social media sites they should do so with responsibility and respect.

If staff wish to set up dedicated social media accounts for their subjects, they should first discuss this with the Marketing team.

8. Monitoring of Internet use

Guesthostname monitors usage of its internet, online content, online services and email services without prior notification or authorisation from users.

Users of email and internet services should have no expectation of privacy in anything they create, store, send or receive using the school's ICT system.

9. Breaches of these guidelines

Any breach of these guidelines that leads to a breach of confidentiality, defamation or damage to the reputation of guesthostname or any illegal acts or acts that render guesthostname liable to third parties may result in legal action, disciplinary action or sanctions in line with the published school policies for staff and pupils.
9.13. Social Media Policy from school 8

Social Media Policy

<table>
<thead>
<tr>
<th>Date of Policy Issue: November 2015</th>
<th>Date of Policy Review: November 2018</th>
</tr>
</thead>
<tbody>
<tr>
<td>Approved by:</td>
<td>Date of Approval: November 2015</td>
</tr>
<tr>
<td>Mrs F Martin</td>
<td></td>
</tr>
<tr>
<td>Head Teacher</td>
<td></td>
</tr>
</tbody>
</table>

This document should be read in conjunction with information contained in the Staff Acceptable Use of ICT Policy which can be found at T\Whole School General\Staff\School Policies & Management Documents\Current Policies and other related policy documents referred to at Appendix 1 below.

The policy sets out the rules and standards to be applied for use of the Internet and social media in Hampshire schools and outlines the risks for both users and schools, as well as the potential consequences of misuse of the Internet and social media. Staff should raise any concerns about e-safety with the Head Teacher.

Introduction

1. It is recognised that social networking has the potential to play an important part in many aspects of school life, including teaching and learning, external communications and continuing professional development. This policy therefore encourages the responsible and professional use of the Internet and social media to support educational delivery and professional development.

2. The Internet provides an increasing range of social media tools that allow users to interact with each other. Whilst recognising the important benefits of these media tools for new opportunities for communication, this policy sets out the principles that school staff, governors and contractors are required to follow when using social media.

3. It is essential that students, parents and the public at large have confidence in the school’s decisions and services. The principles set out in this policy are designed to ensure that staff members use social media responsibly so that confidentiality of students and staff members and the reputation of the school and the County Council are safeguarded. In this context, staff members must be conscious at all times of the need to keep their personal and professional lives separate.

Objectives

The primary objective of this policy is to set out the responsibilities of staff, governors and contractors at the school who use the Internet and social networking sites. It is also aimed at ensuring that the Internet and social media are utilised safely, lawfully and effectively for the successful and economic delivery of school-based services.
Scope

1. This policy applies to the school governing body, all teaching and other staff, whether employed by the County Council or employed directly by the school, external contractors providing services on behalf of the school or the County Council, teacher trainees and other trainees, volunteers and other individuals who work for or provide services on behalf of the school. These individuals are collectively referred to in this policy as staff or staff members.

2. The policy covers personal use of social media as well as the use of social media for official school purposes, including sites hosted and maintained on behalf of the school. It is acknowledged that there is significant potential for the school to exploit the Internet and social media and that this can bring great advantages. The use of both the Internet and social media is therefore actively encouraged.

3. The policy applies to personal workspace such as social networking sites (for example Facebook, MySpace, Yapper), blogs, microblogs such as Twitter, chatrooms, forums, podcasts, open access online encyclopedias such as Wikipedia, social bookmarking sites such as del.icio.us and content sharing sites such as flickr and YouTube. The Internet is a fast moving technology and it is impossible to cover all circumstances or emerging media - the principles set out in this policy must be followed irrespective of the medium.

4. This policy provides a structured approach to using the Internet and social media and will ensure that it is effective, lawful and does not compromise the school's reputation, school information or computer systems/networks.

Risks

The school recognises the risks associated with use of the Internet and social media and regulates their use to ensure this does not damage the school, its staff and the people it serves. Principal amongst these risks are:

- cyber bullying by pupils/students;
- access to inappropriate material;
- offending behaviour toward staff members by other staff or pupils/students;
- other misuse by staff including inappropriate personal use;
- inappropriate behaviour, criticism and complaints from external sources;
- loss or theft of personal data;
- virus or other malware (malicious software) infection from infected sites;
- disclosure of confidential information;
- damage to the reputation of the school;
- social engineering attacks - i.e. the act of manipulating people into disclosing confidential material or carrying out certain actions;
- civil or criminal action relating to breaches of legislation;
- staff members openly identifying themselves as school personnel and making disparaging remarks about the school and/or its policies, about other staff members, pupils or other people associated with the school.

Applying the Policy

Responsibilities of staff members
The following principles apply to online participation and set out the standards of behaviour expected of staff members as representatives of the School.

The School has a duty to provide a safe working environment free from bullying and harassment. If a staff member uses any information and/or communications technology, including email and social networking sites, to make reference to people working at or for the School, or people receiving services from the School then any information posted must comply with all relevant professional Codes of Practice and the School’s ICT Acceptable Use Policy.

Using the Internet and social media for approved school purposes

Staff must ensure that they use the Internet sensibly, responsibly and lawfully and that use of the Internet and social media does not compromise school information or computer systems and networks. They must ensure that their use will not adversely affect the school or its business, nor be damaging to the school’s reputation and credibility or otherwise violate any school policies. In particular:

- the school’s Internet connection is for business use and its use, and use of social networking, must only take place in line with the school’s policies;
- when acting with approval on behalf of the school, under no circumstances may staff comment or contribute unless identifying themselves as school staff;
- personal email or social media accounts must never be used to conduct school business. Any accounts created for this purpose must link to a school email address. The only exception is the use of professional networks (such as LinkedIn), where it is acceptable to use an account linked to a personal email address in both a professional and personal capacity;
- staff members must report any safeguarding issues they become aware of;
- staff members must not cite or reference pupils/students/parents without approval;
- material published must not risk actions for defamation, or be of an illegal, sexual, discriminatory or offensive nature;
- material published must be truthful, objective, legal, decent and honest;
- material published must not breach copyright;
- any publication must comply with all of the requirements of the Data Protection Act 1998, and must not breach any common law duty of confidentiality, or any right to privacy conferred by the Human Rights Act 1998, or similar duty to protect private information;
- material published must not be for party political purposes or specific campaigning which in whole or part appears to affect public support for a political party;
- material published must not be used for the promotion of personal financial interests, commercial ventures or personal campaigns;
- the tone of any publication must be respectful and professional at all times, and material must not be couched in an abusive, hateful, or otherwise disrespectful manner;
- publication must be in line with school policies;
- if used with pupils/students, staff must ensure that the site’s rules and regulations allow the age group to have accounts and that the parents are informed of its use;
- staff members must not use the Internet or social media if doing so could pose a risk (e.g. financial or reputational) to the school, its staff or services or where they do not have the approval from the Senior Leadership Team.
Personal use of internet and social media

The school’s Internet connection is intended primarily for educational use. There is no right for staff to use the Internet for private use and access can be withdrawn at any time. Where staff members are permitted access via the school’s Internet connection:

- the school is not liable for any financial or material loss to an individual user in accessing the Internet for personal use;
- staff wishing to spend significant time outside of their own normal working hours using the Internet – e.g. for study purposes must obtain prior approval;
- inappropriate or excessive use may result in disciplinary action and/or removal of Internet facilities;
- the school will monitor Internet and email use by electronic means, and staff cannot expect privacy when using the school’s Internet facility;
- personal Internet search histories and the content of emails sent for personal use will be accessed by staff only according to the Council’s Internet, Internet and Email Monitoring Policy and School’s disciplinary procedures, and only then when a legitimate concern has been raised by monitoring processes, legitimate concerns expressed by a colleague, or some other legitimate and objective complaint or incident;
- electronic correspondence will only be intercepted in exceptional circumstances.
- users are not permitted to access, display or download from Internet sites that hold offensive material. Offensive material includes, but is not restricted to, hostile text or images relating to gender, ethnicity, race, sex, sexual orientation, religious or political convictions and disability. The school is the final arbiter on what is or is not offensive material or what is or is not acceptable, permissible or excessive use of the Internet – staff concerned about this should refrain from using the Internet for private matters;
- due to the potential impact on school systems, the use of streaming media such as video (YouTube, BBC iPlayer, Vimeo etc.) or audio (internet radio, Spotify, Google Music etc.) should be kept to a minimum. Streaming should be limited to occasional short video/audio clips only. Staff members must not stream TV, films or continual broadcasts (e.g. sport, news, radio or playlists);
- due to the potential impact on school systems, the downloading of media for personal use such as video (YouTube, BBC iPlayer, Vimeo etc.) or audio (internet radio, Spotify, Google Music etc.) is not permitted;
- certain websites will be blocked, but it is a breach of this guide to access any of the following types of site:
  - pornography/Adult /mature content
  - gambling/betting/gaming
  - alcohol/Tobacco
  - illegal drugs
  - auction sites
  - violence/hate/racism
  - weapons
  - any site engaging in or encouraging illegal activity
  - illegal file-sharing sites
- staff members who accidentally or unintentionally access a site containing any prohibited content must leave the site immediately and inform the Senior Leadership Team. Genuine mistakes and accidents will not be treated as breach of this policy;
- staff members may not download software from any source without approval;
- Staff members are not permitted to alter or tamper with their PC Internet settings for the purpose of bypassing or attempting to bypass filtering and monitoring procedures unless they have been given express permission to do so by the Headteacher;
- Staff members must not communicate personal or confidential information via the Internet/Intranet for any purpose, unless expressly authorized to do so by their Senior Leadership Team;
- Users must not create, download, upload or transmit any obscene or indecent images, data or other material, or any data capable of being resolved into obscene or indecent images or material;
- Users must not create, download, upload or transmit any defamatory, sexist, racist, offensive or otherwise unlawful images, data or other material;
- Users must not create, download, upload or transmit material that is designed or would be likely to annoy, harass, bully, inconvenience or cause anxiety to others;
- Users must not create, download, upload or transmit any unsolicited commercial or bulk webmail, chain letters or advertisements;
- Users must not download any digital media including music, images, photos and video that would be in breach of copyright or licensing arrangements, or where copyright or ownership cannot be determined;
- The use of file sharing services or software is prohibited for any purpose;
- The use of cloud storage e.g. Google Drive, Dropbox, SkyDrive, iCloud, is not permitted for the storage of sensitive personal data.

School reputation and confidentiality

The school recognizes an employee’s right to a private life. However the school must also ensure its reputation and confidentiality are protected. Therefore an employee using any ICT away from school, including email and social networking sites must:

- Refrain from identifying themselves as working for the school in a way that could have the effect of bringing the school into disrepute;
- Not express a personal view as a school employee that the school would not want to be associated with;
- Notify the Senior Leadership Team immediately if they consider that content posted via any information and communications technology, including emails or social networking sites, conflicts with their role in the school;
- Not have any unauthorised contact or accept ‘friend’ requests through social media with any pupil/student under the age of 18 (or under age 19 where the school has such provision), (including former pupils/students and/or those who attend other schools) unless they are family members;
- Exercise caution when having contact or accepting ‘friend’ requests through social media with parents so as not to compromise the school’s reputation or school information;
- Not allow interaction through information and communications technology, including emails or social networking sites, to damage relationships with work colleagues in the school and/or partner organisations, pupils/students or parents;
- Not disclose any data or information about the school, colleagues in the school and/or partner organisations, pupils/students or parents that could breach the Data Protection Act 1998;
- Not use the Internet or social media in or outside of work to bully or harass other staff or others.
Personal Information

School staff must never give out personal details of others, such as home address and telephone numbers. Staff must handle all personal or sensitive information in line with the school’s Data Protection Policies.

With the rise in identity theft and fraud, staff may wish to consider the amount of personal information that they display on personal profiles.

Cyber bullying and Harassment

The use of ICT in relation to Bullying and Harassment

i. This section should be read in conjunction with the guidance contained in "Cyber-bullying: Practical Advice for School Staff". Cyber Bullying and Cyber Harassment, like other forms of bullying and harassment, imply a relationship where an individual has some influence or advantage that is used improperly over another person or persons, where the victim(s) is subjected to a disadvantage or detriment, and where the behaviour is unwarranted and unwelcome to the victim. However, in this case the technological environment has meant that the acts of bullying and harassment now include the use of information and communications technology including email and social networking.

ii. The school will consider it a potential disciplinary matter if users utilise any information and communications technology, including email and social networking sites, in such a way as to bully/harass others in the school or in partner organisations, or pupils/students or parents, whether this takes place during or outside of work. Staff members need to be aware that no matter what the privacy settings on their social media/networking site, inappropriate/derogatory information about a colleague in the school or partner organisations, pupils or parents, can find its way into the public domain even when not intended.

iii. It should be noted that a person does not need to directly experience this form of victimisation in order for it to be classed as cyber bullying/harassment. The fact that a person is unaware that offensive or derogatory comments about them have been placed on websites still fits the criteria of cyber bullying/harassment.

iv. If a staff member receives any threats, abuse or harassment from members of the public through their use of social media then they must report such incidents using the school’s procedures. Support is also available through Hampshire’s confidential counselling service, Employee Support (0800 030 5182).

Senior Leadership responsibility in relation to Bullying and Harassment

a. The school owes a duty to take reasonable steps to provide a safe working environment free from bullying and harassment.
b. For this reason, it is essential that the Senior Leadership Team take appropriate steps to deal with any incident where it is alleged that a staff member has subjected others to abusive or personally offensive emails, phone calls or content on social networking sites such as Facebook, Twitter, or by any other means.

c. If a Senior Leader is made aware of such an allegation, the Senior Leadership Team should deal with it in the same way as any other incident of bullying or harassment in line with school policies, by investigating the allegations promptly and appropriately and providing the victim with appropriate support to demonstrate that the matter is being dealt with seriously.

d. Senior Leaders should encourage staff to preserve all evidence by not deleting emails, logging phone calls and taking screen prints of websites. If the incident involves illegal content or contains threats of a physical or sexual nature, the Senior Leadership team should consider advising the employee that they should inform the police. In the event that such evidence contains indecent images of children, it is an offence to save, send, or alter an image or to show it to anyone else. Therefore, the evidence must be placed in a secure location such as a locked cupboard where others will not be able to see it. In these circumstances the Police should be contacted immediately for advice.

Signature

It will be normal practice for staff to read and sign a declaration as outlined in Appendix 2, to confirm that they have had access to the School Social Media Policy and that they accept and will follow its terms.

Staff must comply with the terms of this policy. Any breach will be considered to be a breach of disciplinary rules, which may lead to a disciplinary sanction (e.g. warning), dismissal, and/or withdrawal of access to ICT facilities. Staff should be aware, that in certain instances, inappropriate use of Social Media may become a matter for police or social care investigations.
Appendix 1

Legal and Policy Framework

The School is committed to ensuring that all staff members provide confidential services that meet the highest standards. All individuals working on behalf of the school are bound by a legal duty of confidence and other laws to protect the confidential information they have access to during the course of their work. Disclosure of confidential information on social media is likely to be a breach of a number of laws and professional Codes of Conduct, including the following:

- Human Rights Act 1998
- Common law duty of confidentiality
- Data Protection Act 1998, and
- Employment Practices Data Protection Code

Confidential information includes, but is not limited to:

- Person-identifiable information, e.g. pupil and employee records protected by the Data Protection Act 1998
- Information divulged in the expectation of confidentiality
- School or County Council business or corporate records containing organisationally or publicly sensitive information
- Any commercially sensitive information such as information relating to commercial proposals or current negotiations, and
- Politically sensitive information.

Staff members should also be aware that other laws relating to libel, defamation, harassment and copyright may apply to information posted on social media, including:

- Libel Act 1843
- Protection from Harassment Act 1997
- Criminal Justice and Public Order Act 1994
- Malicious Communications Act 1998
- Communications Act 2003, and
- Equality Act 2010

Related Policies

The Social Media policy should be read in conjunction with other relevant school and County Council policies, procedures and Codes of Conduct including:

- Staff Acceptable Use of ICT Policy
- Cyber bullying: Practical Advice for School Staff
- Disciplinary Procedures
- Equalities Policy
Appendix 2

Staff Declaration

I have read and understand the School Social Media Policy and understand that inappropriate use may be considered to be misconduct or gross misconduct and may, after proper investigation, lead to a disciplinary sanction or dismissal. I understand that, in certain circumstances, inappropriate use of Social Media may become a matter for police or social care investigations. I understand that if I need any clarification regarding my use of Social Media, I can seek such clarification from any member of the Senior Leadership Team.

Signed: ........................................................................................................

Name: ...........................................................................................................

Date: ............................................................................................................
9.14. **Staff Acceptable Use of ICT - November 2015 from school 8**

---

### Staff Acceptable Use of ICT

<table>
<thead>
<tr>
<th>Date of Policy Issue: November 2015</th>
<th>Date of Policy Review: November 2018</th>
</tr>
</thead>
</table>

#### 1.0 Introduction

1.1 This policy is based on the Hampshire County Council model for Hampshire maintained schools. The policy has been further developed for [insert school name]. This policy should be read in conjunction with other relevant school and County Council policies, procedures and Codes of Conduct including:

- School Social Media Policy
- Information Security – Corporate Acceptable Use Policy
- Email, Internet and Intranet Monitoring Policy
- Cyber bullying: Practical Advice for School Staff
- Disciplinary Procedure

#### 1.2 Staff should recognise and report any potential misuse

#### 2.0 Application

2.1 This policy applies to the Governing Body, all teaching and other staff, whether employed by the County Council or employed directly by the school, external contractors providing services on behalf of the school or the County Council, teacher trainees and other trainees, volunteers and other individuals who work for or provide services on behalf of the school. These individuals are collectively referred to in this policy as staff or staff members.

2.2 The policy applies in respect of all ICT resources and equipment within the school and resources that have been made available to staff for working at home. ICT resources and equipment includes computer resources, use of school internet access and email systems, software (including use of software such as SAP and SIMS), school telephones and text systems, cameras and recording equipment, intranet and virtual learning environment and any other electronic or communication equipment used in the course of the employee or volunteer’s work.

2.2 This policy also provides advice to staff in respect of the potential risks and consequences in relation to inappropriate use of their own personal ICT facilities, where this use is inconsistent with the expectations of staff working with children and young people.
to nominated staff and unless permission and access has been provided, staff must not access these systems.

3.4 Some staff may be provided with laptops and other equipment for the performance of their role. Where provided, staff must ensure that their school laptop/equipment is not accessible by others when in use at home and that it is not used inappropriately by themselves or others. Staff must also ensure that they bring their laptop/equipment in as required for updating of software, licences and virus protection.

3.5 Where the school provides digital cameras and other recording equipment for educational and school business use and it is used away from the school site, it must be kept secure and safe. Where pictures of pupils are taken, staff must ensure that they ensure consent has been provided by parents, and that the school’s policy in relation to use of pictures, is followed.

3.6 If the school does not provide school mobile phones, staff may use, in urgent or emergency situations during off site visits, their personal mobile telephones. Where used in these emergency situations and a cost incurred, the school will provide reimbursement of the cost of any calls made. Should staff need to make contact whilst off site, this should normally be undertaken via the school rather than a direct call from the individual’s personal mobile. School staff who have access to colleagues’ personal contact details must ensure that they are kept confidential.

3.7 No mobile telephones or similar devices, even those with hands free facilities should be used whilst driving on school business.

3.8 Whether school staff have access to the school telephone system for personal use will be confirmed by the school. Where such use is made of this facility, it must be done during break periods, must not be excessive and the school should require either the cost of the call or a donation to be made towards the cost of the call.
3.9 The will ensure that Display Screen Equipment assessments are undertaken by staff using computers frequently for work, and not for infrequent short periods of time during the course of the day, in accordance with our Health and Safety Policy.

4.0 Communication with parents, pupils and governors

4.1 The communicates with parents and governors through a variety of mechanisms. The points below highlight who is normally authorised to use which systems and can directly communicate without requiring any approval before use or to agree content. We will indicate to staff if any other staff are permitted to make contact using the systems below:

4.1.1 School Telephones – all teachers, administrative staff and staff who have been permitted through their roles in pupil welfare or a home/school link staff. Normally teaching assistants and lunchtime supervisory staff would need to seek approval from a member of the senior leadership team where they feel they need to make a telephone call to a parent.

4.1.2 Text System - Office staff. Where other staff need to send a text, this will normally be approved by a member of the Senior Leadership Team.

4.1.3 Letters – Normally all teachers may send letters home, but they may be required to have those approved by the Head Teacher before sending. Where office staff send letters home, these will normally require approval by the School Business Manager/Head Teacher.

4.1.4 Email – school email accounts should not be used for communication with parents unless this is part of their normal role, e.g. Tutor, Progress Leader, Senior Leadership Team and administrative staff. Other staff should seek approval from a member of the senior leadership team. Email is used as a normal method of communication amongst school governors and where governors are linked in particular areas with members of staff, communication may take place via email.

4.1.5 Visits home – All home visits are normally subject to approval by the senior leadership team and must follow the school’s policy on home visits.

4.2 Under normal circumstances, school staff should not be using any of the methods outlined above to communicate directly with pupils. If a member of staff needs to contact a pupil direct via any of these methods, this must be approved by the Head Teacher.

4.3 Where pupils are submitting work electronically to school staff, this must be undertaken using school systems and not via personal email.

5.0 Social Media

5.1 School staff are advised to exercise extreme care in their personal use of social networking sites, giving consideration to their professional role working with children.
Staff should make appropriate use of the security settings available through social networking sites and ensure that they keep them updated as the sites change their settings. Staff are advised that inappropriate communications that come to the attention of the school can lead to disciplinary action, including dismissal.

5.2 Staff should refer to the School Social Media Policy which contains detailed advice on the expectations of staff when using social media.

6.0 Unacceptable Use

6.1 Appendix 1 provides a list of Do’s and Don’ts for school staff to enable them to protect themselves from inappropriate use of ICT resources and equipment. School systems and resources must not be used under any circumstances for the following purposes:

6.1.1 to communicate any information that is confidential to the school or to communicate/share confidential information which the member of staff does not have authority to share;

6.1.2 to present any personal views and opinions as the views of the school, or to make any comments that are libellous, slanderous, false or misrepresent others;

6.1.3 to access, view, download, post, email or otherwise transmit pornography, sexually suggestive or any other type of offensive, obscene or discriminatory material;

6.1.4 to communicate anything via ICT resources and systems or post that may be regarded as defamatory, derogatory, discriminatory, harassing, bullying or offensive, either internally or externally;

6.1.5 to communicate anything via ICT resources and systems or post that may be regarded as critical of the school, the leadership of the school, the school’s staff or its pupils;

6.1.6 to upload, download, post, email or otherwise transmit or store material that contains software viruses or any other computer code, files or programmes designed to interrupt, damage, destroy or limit the functionality of any computer software or hardware or telecommunications equipment;

6.1.7 to collect or store personal information about others without direct reference to The Data Protection Act;

6.1.8 To use the school’s facilities to undertake any trading, gambling, other action for personal financial gain, or political purposes, unless as part of an authorised curriculum project;

6.1.9 to visit or use any online messaging service, social networking site, chat site, web based email or discussion forum not supplied or authorised by the school;
6.1.10 to undertake any activity (whether communicating, accessing, viewing, sharing, uploading or downloading) which has negative implications for the safeguarding of children and young people;

6.2 Any of the above activities are likely to be regarded as gross misconduct, which may, after proper investigation, lead to dismissal. If employees are unsure about the use of ICT resources including email and the intranet, advice should be sought from a member of the Senior Leadership Team or ICT lead if applicable.

6.3 Where an individual accidently or unintentionally accesses a website or material that contains any prohibited content, they must leave the site immediately and inform the Headteacher or other member of the senior leadership team. Schools are encouraged to use appropriate blocking software to avoid the potential for this to happen. Reporting to the Headteacher or senior leadership team equally applies where school staff are using school equipment or facilities at home and accidentally access inappropriate sites or material. Genuine mistakes and accidents will not be treated as a breach of this policy.

6.4 Where an individual has been communicated with in a manner outlined above (e.g. has received an inappropriate email or attachment), they are advised to report this immediately to the Head Teacher or another member of the senior leadership team so that this can be dealt with appropriately.

7.0 Personal and private use

7.1 All staff with access to computer equipment, including email and internet, are permitted to use them for occasional personal use provided that this is access is not:

7.1.1 taking place at the expense of contracted working hours (i.e. is not taking place during paid working time)

7.1.2 interfering with the individual’s work

7.1.3 relating to a personal business interest

7.1.4 involving the use of news groups, chat lines or similar social networking services

7.1.5 at a cost to the school

7.1.6 detrimental to the education or welfare of pupils at the school.

7.2 Excessive personal use of school facilities is likely to be considered to be a disciplinary matter, may lead to restricted access to computer equipment and where costs are incurred (e.g. personal telephone use), the school will seek reimbursement from the member of staff.

7.3 It is important for staff to also be aware that inappropriate use of their own personal or other ICT facilities in their personal time, can have implications for their employment
7.4 Where staff have brought their own personal equipment such as mobile telephones, digital assistants, laptops and cameras, into the school, these personal items, should not be used during pupil contact sessions unless authorised. Staff should follow all points outlined in this section in relation to their personal use. Staff should ensure that there is no inappropriate content on any of these pieces of equipment and ensure that they are not accessed by pupils at any time. Such equipment should not normally be required to enable staff to undertake their role but where it is used, staff should take care to ensure any school data/images are deleted following use of the equipment.

7.5 Whilst individuals may be required to use their personal mobile telephone to make contact with the school, staff should exercise care and seek reimbursement as outlined in section 3.

8.0 Security and confidentiality

8.1 Any concerns about the security of the ICT system should be raised with a member of the senior leadership team.

8.2 Staff are required to ensure that they keep any passwords confidential, do not select a password that is easily guessed and regularly change such passwords.

8.3 Staff must take account of any advice issued regarding what is permitted in terms of downloading educational and professional material to the school server. Where staff are provided with a memory pen for such activity, to both protect the integrity of the server and to save space, this should be used. All staff must review the appropriateness of the material that they are downloading prior to downloading and are encouraged to do so from known and reputable sites to protect the integrity of the school’s systems. Where problems are encountered in downloading material, this should be reported to the school’s ICT lead.

8.4 Where staff are permitted to work on material at home and bring it in to upload to the school server through their memory pens, they must ensure that they have undertaken appropriate virus checking on their systems. Where provided, staff should normally use their school issued laptop for such work.

8.5 Staff must ensure that they follow appropriate and agreed approval processes before uploading material for use by pupils to the pupil ICT system.

8.6 Whilst any members of school staff may be involved in drafting material for the school website, staff must ensure that they follow appropriate and agreed approval processes before uploading material to the website.

8.7 The school will nominate staff who are responsible for ensuring that all equipment is regularly updated with new software including virus packages and that licences are maintained on all school based and school issued equipment. Staff must ensure that
they notify the nominated staff when reporting any concerns regarding potential viruses, inappropriate software or licences.

8.8 Staff must ensure that their use of the school’s ICT facilities does not compromise rights of any individuals under the Data Protection Act. This is particularly important when using data off-site and electronic data must only be taken off-site in a secure manner, either through password protection on memory pens or through encrypted memory pens. This is also particularly important when communicating personal data via email rather than through secure systems. In these circumstances, staff must ensure that they have the correct email address and have verified the identity of the person that they are communicating the data with.

8.9 Staff must also ensure that they do not compromise any rights of individuals and companies under the laws of Copyright through their use of ICT facilities.

9.0 Monitoring

9.1 The School and Hampshire County Council’s ICT Services and therefore is required to comply with their email, internet and Intranet policies.

9.2 The school and county council reserve the right to monitor the use of email, internet and Intranet communications and where necessary data may be accessed or intercepted in the following circumstances:

9.2.1 to ensure that the security of the school and county council’s hardware, software, networks and systems are not compromised

9.2.2 to prevent or detect crime or unauthorised use of the school or county council’s hardware, software, networks or systems

9.2.3 to gain access to communications where necessary where a user is absent from work

9.3 Where staff have access to the internet during the course of their work, it is important for them to be aware that the school or county council may track the history of the internet sites that have been visited.

9.4 To protect the right to privacy, any interception of personal and private communications will not take place unless grounds exist to show evidence of crime, or other unlawful or unauthorised use. Such interception and access will only take place following approval by the Chair of Governors, after discussions with relevant staff in Hampshire County Council’s HR, IT and Audit Services and following an assessment to determine whether access or interception is justified.

10.0 Whistleblowing and cyberbullying

10.1 Staff who have concerns about any abuse or inappropriate use of ICT resources, virtual learning environments, camera/recording equipment, telephony, social networking sites, email or internet facilities or inappropriate communications, whether by pupils or
colleagues, should alert the Head Teacher to such abuse. Where a concern relates to the Headteacher, this should be disclosed to the Chair of Governors. If any matter concerns child safety, it should also be reported to the Designated Safeguarding Lead (DSL).

10.2 It is recognised that increased use of ICT has led to cyberbullying and/or concerns regarding e-safety of school staff. Staff are strongly advised to notify their Head Teacher where they are subject to such circumstances. Advice can also be sought from professional associations and trade unions. Support is also available through Hampshire’s confidential counselling service, Employee Support (0800 080 5182) and also via the UK Safer Internet Centre helpline@saferinternet.org.uk or 0844 381 4772.

10.3 Further advice on cyberbullying and harassment can be found in the School Social Media Policy and in Cyber bullying: Practical Advice for School Staff.

11.0 Signature

11.1 Staff must read and sign the declaration in Appendix 2, to confirm that they have had access to the acceptable use policy and that they accept and will follow its terms.

11.2 Staff must comply with the terms of this policy. Any breach will be considered to be a breach of disciplinary rules, which may lead to a disciplinary sanction (e.g. warning), dismissal, and/or withdrawal of access to ICT facilities. Staff should be aware that in certain instances, inappropriate use of ICT may become a matter for police or social care investigations.
Do’s and Don’ts: Advice for Staff

Whilst the wide range of ICT systems and resources available to staff, both in school and outside of school, have irrefutable advantages, there are also potential risks that staff must be aware of. Ultimately if staff use ICT resources inappropriately, this may become a matter for a police or social care investigation and/or a disciplinary issue which could lead to their dismissal. Staff should also be aware that this extends to inappropriate use of ICT outside of school.

This Dos and Don’ts list has been written as a guidance document. Whilst it is not fully comprehensive of every circumstance that may arise, it indicates the types of behaviours and actions that staff should not display or undertake as well as those that they should in order to protect themselves from risk.

General issues

Do

- ensure that you do not breach any restrictions that there may be on your use of school resources, systems or resources
- ensure that where a password is required for access to a system, that it is not inappropriately disclosed
- respect copyright and intellectual property rights
- ensure that you have approval for any personal use of the school’s ICT resources and facilities
- be aware that the school’s systems will be monitored and recorded to ensure policy compliance
- ensure you comply with the requirements of the Data Protection Act when using personal data
- seek approval before taking personal data off the school site
- ensure personal data is stored safely and securely whether kept on site, taken off site or accessed remotely
- report any suspected misuse or concerns that you have regarding the school’s systems, resources and equipment to the Headteacher or designated manager and/or Designated Safeguarding Lead as appropriate
- be aware that a breach of your school’s Acceptable Use Policy will be a disciplinary matter and in some cases, may lead to dismissal
- ensure that any equipment provided for use at home is not accessed by anyone not approved to use it
- ensure that you have received adequate training in ICT
- ensure that your use of ICT bears due regard to your personal health and safety and that of others

Appendix 1
Don't

• access or use any systems, resources or equipment without being sure that you have permission to do so
• access or use any systems or resources or equipment for any purpose that you don't have permission to use the system, resources or equipment for
• compromise any confidentiality requirements in relation to material and resources accessed through ICT systems
• use systems, resources or equipment for personal use without having approval to do so

• use other people's log on and password details to access school systems and resources
• download, upload or install any hardware or software without approval
• use unsecure removable storage devices to store personal data
• use school systems for personal financial gain, gambling, political activity or advertising
• communicate with parents and pupils outside normal working hours unless absolutely necessary
Use of email, the internet, school and HCC intranets

Do
- alert your Headteacher or designated manager if you receive inappropriate content via email
- be aware that the school's email system will be monitored and recorded to ensure policy compliance
- ensure that your email communications are compatible with your professional role
- give full consideration as to whether it is appropriate to communicate with pupils or parents via email, or whether another communication mechanism (which may be more secure and where messages are less open to misinterpretation) is more appropriate
- be aware that the school may intercept emails where it believes that there is inappropriate use
- seek support to block spam
- alert your Headteacher or designated manager if you accidentally access a website with inappropriate content
- be aware that a website log is recorded by the school and will be monitored to ensure policy compliance
- answer email messages from pupils and parents within your directed time
- mark personal emails by typing 'Personal/Private' within the subject header line

Don't
- send via email or download from email, any inappropriate content
- send messages that could be misinterpreted or misunderstood
- use personal email addresses to communicate with pupils or parents
- send messages in the heat of the moment
- send messages that may be construed as defamatory, discriminatory, derogatory, offensive or rude
- use email systems to communicate with parents or pupils unless approved to do so
- download attachments from emails without being sure of the security and content of the attachment
- forward email messages without the sender's consent unless the matter relates to a safeguarding concern or other serious matter which must be brought to a senior manager's attention
- access or download inappropriate content (material which is illegal, obscene, libellous, offensive or threatening) from the internet or upload such content to the school or HCC intranet
- upload any material onto the school website that doesn't meet style requirements and without approval

Use of telephones, mobile telephones and instant messaging

Do
- ensure that your communications are compatible with your professional role
- ensure that you comply with your school's policy on use of personal mobile telephones
- ensure that you reimburse your school for personal telephone calls as required

Don't
- use school mobile telephones when on educational visits
Don’t
• send messages that could be misinterpreted or misunderstood
• excessively use the school’s telephone system for personal calls

Use of cameras and recording equipment

Do
• ensure that material recorded is for educational purposes only
• ensure that where recording equipment is to be used, approval has been given to do so
• ensure that material recorded is stored appropriately and destroyed in accordance with the school’s policy
• ensure that parental consent has been given before you take pictures of school pupils

Don’t
• bring personal recording equipment into school without the prior approval of the Headteacher
• inappropriately access, view, share or use material recorded other than for the purposes for which it has been recorded
• put material onto the VLE, school intranet or intranet without prior agreement from a member of senior staff

Use of social networking sites

Do
• ensure that you understand how any site you use operates and therefore the risks associated with using the site
• familiarise yourself with the processes for reporting misuse of the site
• consider carefully who you accept as friends on a social networking site
• report to your Headteacher any incidents where a pupil has sought to become your friend through a social networking site
• take care when publishing information about yourself and images of yourself online — assume that anything you release will end up in the public domain
• ask yourself about whether you would feel comfortable about a current or prospective employer, colleague, pupil or parent viewing the content of your page

Don’t
• follow school procedures for contacting parents and/or pupils
• only contact pupils and/or parents via school based computer systems
• through your teaching, alert pupils to the risk of potential misuse of social networking sites (where employed in a teaching role)
Don't

- spend excessive time utilising social networking sites while at work
- accept friendship requests from pupils – you may be giving them access to personal information, and allowing them to contact you inappropriately
- put information or images on line or share them with colleagues, pupils, or parents (either on or off site) when the nature of the material may be controversial
- post anything that may be interpreted as slanderous towards colleagues, pupils or parents
- use social networking sites to contact parents and/or pupils
Staff Code of Conduct for ICT

To ensure that members of staff are fully aware of their professional responsibilities when using information systems and when communicating with parents, pupils and others, they are asked to sign this code of conduct. Staff should consult the detail of the school’s Policy for Staff Acceptable Use of ICT for further information and clarification.

- I appreciate that ICT includes a wide range of system, including mobile phones, personal digital assistants, cameras, email, Internet and HCC Intranet access and use of social networking and that ICT use may also include personal ICT devices when used for school business.
- I understand that it may be a criminal offence to use the school ICT system for a purpose not permitted.
- I understand that I must not communicate information which is confidential to the school or which I do not have the authority to share.
- I understand that school information systems and hardware may not be used for personal or private without the permission of the Headteacher.
- I understand that my use of school information systems, Internet and email may be monitored and recorded, subject to the safeguards outlined in the policy to ensure policy compliance.
- I understand the level of authority required to communicate with parents and pupils using the various methods of communication.
- I understand that I must not use the school ICT system to access inappropriate content.
- I understand that accessing, viewing, communicating and downloading material which is pornographic, offensive, defamatory, derogatory, harassing or bullying is inappropriate use of ICT.
- I will respect system security and I will not disclose any password or security information to anyone other than an authorised system manager. I will not use anyone’s account except my own.
- I will not install any software or hardware without permission.
- I will follow the school’s policy in respect of downloading and uploading of information and material.
- I will ensure that personal data is stored securely and is used appropriately whether in school, taken off the school premises or accessed remotely. I will not routinely keep personal data on removable storage devices. Where personal data is required, it will be password protected/encrypted and removed after use.
- I will respect copyright, intellectual property and data protection rights.
- I understand use for personal financial gain, gambling, political activity, advertising or illegal purposes is not permitted.
- I will report any incidences of concern regarding children’s safety to the Designated Safeguarding Lead or Headteacher.
• I will report any incidences of inappropriate use or abuse of ICT and inappropriate electronic communications, whether by pupils or colleagues, to the Headteacher, or if appropriate, the Chair of Governors.

• I will ensure that any electronic communication undertaken on behalf of the school, including email and instant messaging are compatible with my professional role and that messages do not present personal views or opinions and cannot be misunderstood or misinterpreted.

• I understand the school’s stance on use of social networking and given my professional role working with children, will exercise care in any personal use of social networking sites.

• I will ensure that any electronic communications with pupils, where permitted, are compatible with my professional role and that messages cannot be misunderstood or misinterpreted.

• I will promote e-safety with pupils in my care and help them to develop a responsible attitude to system use, communication and publishing.

• I understand that inappropriate use of personal and other non-school based ICT facilities can have implications for my employment at the school where this becomes known and where activities undertaken are inconsistent with expectations of staff working with children.

The school may exercise its right to monitor the use of the school’s ICT systems and accesses, to intercept email and to delete inappropriate materials where it believes unauthorised use of the school’s ICT systems may be taking place, or the system may be being used for criminal purposes or for storing unauthorised or unlawful text, images or sound.

I have read and understand the Policy for Staff Acceptable Use of ICT and understand that inappropriate use may be considered to be misconduct or gross misconduct and may, after proper investigation, lead to a disciplinary sanction or dismissal. I understand that if I need any clarification regarding my use of ICT facilities, I can seek such clarification from any member of the Senior Leadership Team.

SIGNED: ........................................................................

DATE: ........................................................................

NAME (PRINT): ..................................................................