Network Policy & E-Safety	
Policy area	ICT
Policy Author	Peter Robinson, IT Manager
Status	Draft/ Approved
Category	Trust Wide/ School Specific
Implementation Date	Autumn Term 24
Review cycle	Annual
Next review date	Autumn Term 25
Related policies/ documents	

Document Control

Date	Version	Comments
13/09/2024	V1	
23/10/2024	V2	Approved by Governors

Contents

1 Guidance for using Worthing High School Network and Internet Resources

Networked resources, as well as internet access, Google Drive, Google Classroom and Office 365, are potentially available to students and staff in the school. All users are required to follow the conditions laid down in the policy. Any breach of these conditions may lead to withdrawal of the user's access and in some instances could lead to criminal prosecution. Any breach of the conditions will also be considered a disciplinary matter.

These networked resources are intended for educational purposes and may only be used for legal activities consistent with the policies of the school. Any expression of a personal view about the school or Trust matters in any electronic form of communication must be endorsed to that effect. Any use of the network that would bring the name of the school or Trust into disrepute is not allowed.

The school expects that staff will use new technologies as appropriate within the curriculum and that staff will provide guidance and instruction to pupils in the use of such resources. Independent pupil use of the internet, school email or the school's intranet will only be permitted upon the receipt of a signed permission and agreement form. All computer systems will be regularly monitored to ensure that they are being used in a reasonable fashion.

The IT Department and Senior Leadership Team have the right to monitor files and emails on the school's computer network.

2 Conditions of Use

2.1 Personal Responsibility

Access to the networked resources is a privilege, not a right. Users are responsible for their behaviour and communications. Staff and students will be expected to use the resources for the purposes for which they are made available. Users are to take due care with the physical security of hardware they are using. Users will accept personal responsibility for reporting any misuse of the network to the IT Manager.

3 Acceptable Use

Users are expected to utilise the network systems in a responsible manner. It is not possible to set hard and fast rules about what is and what is not acceptable, but the following list provides some guidelines on the matter:

3.1 Unacceptable Use:

- Accessing or creating, transmitting, displaying or publishing any material (e.g., images, sounds or data) which is likely to cause offence, inconvenience or needless anxiety.
- Accessing or creating, transmitting, displaying or publishing any defamatory material.
- Receiving, sending or publishing material that violates copyright© laws or Data Protection Acts.
- Transmitting unsolicited material to other users (including those on other networks).
- Unauthorised access to data and resources on the school network system or other systems

- User action that would cause corruption or destruction of other user's data, or violate the privacy of other users, or intentionally waste time or resources on the network or elsewhere.

3.2 Additional Guidelines

- You must comply with the acceptable use policy of any other networks that you access, including the Wireless Network for Staff and Guests.
- You must not download or install software without approval from the school's IT Department or attempt to run software programs from a memory stick or portable USB device.
- You shouldn't rely on the school Email facilities for your private correspondence. Signing up to online shopping accounts or social media accounts with your school email is not permitted unless for school use.

4 Network Etiquette and Privacy

Users are expected to abide by the rules of network etiquette. These rules include, but are not limited to, the following:

- Be polite: never send or encourage others to send abusive messages.
- Use appropriate language: users should remember that they are representatives of the school on a global public system. Illegal activities of any kind are strictly forbidden.
- Privacy: do not reveal any personal information (e.g., home address, telephone number) about yourself or other users. Do not trespass into other user's files or folders. Password – do not reveal your password to anyone. Staff users are required to use 'strong' passwords (min 8 characters in length and including numbers and letters, upper and lower case) for the school computer network e.g., tEachEr72, and for this to be changed every 6 months.
- Electronic mail is not guaranteed to be private. Messages relating to or in support of illegal activities will be reported to the authorities. Do not send anonymous messages.
- Disruptions: do not use the network in any way that would disrupt use of the network by others.
- Other considerations: be brief in your notes, cite references for any facts you present. g) Do not attempt to 'hack' the network by accessing areas or files you are not permitted to access.
- Do not try and bypass the filtering systems by using VPNs or other proxies.
- Do not attempt to use command line or PowerShell utilities
- The school network is not to be used for online games.

5 Services

There will be no warranties of any kind, whether expressed or implied, for the network service offered by the school. The school will not be responsible for any damages suffered while on the system. These damages include loss of data as a result of delays, non-deliveries, or service interruptions caused by the system or your errors or omissions. Use of any information obtained via the network is at your own risk.

6 Security

Users are expected to inform the IT Manager immediately a security problem is identified. Do not demonstrate this problem to other users. Users must login with their own user identification and password and must not share this information with other users. Users identified as a security risk will be denied access to the network.

7 Willful Damage

Any malicious attempt to harm or destroy any equipment or data of another user or network connected to the school system will result in loss of access, disciplinary action and if appropriate, legal referral. This includes the creation or uploading of computer viruses. The use of software from unauthorised sources is prohibited.

8 Media Publications

- Named images of students must not be published unless parental permission has been obtained (e.g., photographs, videos, TV presentations, web pages etc.).
- Student's work will only be published (e.g., photographs, videos, TV presentations, web pages etc.) if parental consent has been given.

9 Using the School Network

- All Teachers logged on to the network can reset student passwords via: 'Reset Student Password' icon on the desktop. Find the student by typing their surname. The password will be reset to Worthing1 and the student will be required to change it at login.
- Before you use the network with a class or a club for the first time, check if any of the pupils do not have approved internet access.
- If a pupil's password does not work and you cannot reset it yourself, please email the IT Helpdesk with the student or students name(s)
- All pupils should only use their own accounts when logging on to the network and be reminded to KEEP THEIR PASSWORDS CONFIDENTIAL.
- Each Teacher Desk PC has AB Tutor installed, a piece of software that can be opened by choosing the icon on the taskbar. The teacher logs in with their normal login credentials. This is a tool that will enable the teacher to control and monitor students' activities on PCs. From temporarily blocking internet access or only allowing Microsoft Office programs to work.
- Teachers are allowed access to student's home directories but require permission from either the IT Manager or a member of the senior leadership team to have this facility on their user account.

10 Photographic Images

School trips or special events are commonly situations where photography by pupils and staff should be encouraged to create a meaningful record of those events. There are however, risks involved in creating these images.

One potential risk is that an allegation is made that a member of staff has taken an inappropriate photograph or video during the event. Staff should not use personally owned cameras at all and must always use school owned cameras including school memory cards.

If the member of staff used a personal camera it would be significantly more difficult for them to prove that any allegations were unfounded. With school equipment there is at least a clear demonstration that the photography was consistent with school policy.

Staff should also take steps to handle any images, once created, in an appropriate way. Memory cards, USB drives and CDs should only be used as temporary storage for transport. (Also see the section on Laptop Security – for details on the security of data, including images being transported on portable devices.)

Images must not be taken home and stored or processed on a personally owned computer as it is difficult to maintain control of how they are used and by whom. In the event of any allegation, it would also be more difficult to prove the images were used only in an appropriate fashion. Staff should avoid using personally owned computer equipment and always use school owned equipment for these purposes.

11 Using the Internet in the classroom

The Internet is tremendously powerful, purposeful and beneficial to both pupils and staff in schools. The vast majority of it is perfectly safe to use in schools as a result of school Internet Filtering.

However, as with so many things, there is always an element of risk; even an innocent search can occasionally turn up links to adult content or images. This is especially true within Internet searches, which show inappropriate page “descriptions” in their lists even when the pages themselves are blocked.

To protect staff and pupils alike planning and preparation is vital when using online material in the classroom. By far the safest approach is to test sites on the school system before use.

To be practical, the sites have to be checked in school, through the school filters. Purely testing at home may result in attempting to use a site that is available at home but blocked when you get to the classroom. All too often sites have an acceptable outward looking appearance and this aspect may well be useful for education. However, hazards beneath these outer pages, which cannot be separated by the filters, result in them needing to be blocked.

For younger pupils, it may be safer to direct them to specific, pre-approved websites and avoid using search engines. Alternatively, staff may choose to only use Safer, child friendly search engines such as “CBBC Safe Search” or use pre checked search terms. Naturally, when choosing activities or search terms to be used staff will need to bear in mind the: age, ability and maturity of all pupils as well as any individual student requirements within the class.
If inappropriate material is discovered then turn off the monitor, reassure the pupils and to protect yourself you need to log and report the complete URL to a member of I.T. Support Team or the senior leadership team according to the schools e-Safety policy. This can then be used to ensure, as far as possible, that the material is blocked by the filters.

Avoid printing or capturing any material especially if it is thought it may be illegal. Any suspected illegal material should be reported immediately.

12 Use of school mobile devices

Personal use of technology by staff has been shown to increase both confidence and competence with using that technology in a professional capacity. Again, as in all activities, there are risks that need to be mitigated.

The risks include, but they are not limited to:

- Access to wider sites by family members, for instance a gaming site or Internet shopping, would increase the possibility of virus attack and identity theft.
- Access to confidential information stored on the laptop or peripheral devices by family members or friends.
- A very few members of staff, or members of their household, may feel that viewing inappropriate, "adult material" via a school laptop whilst at home is acceptable in their own time. It is certainly not.

Note: There has been a case where such material was accidentally seen in a school as a result of such activity. Naturally cases of this type of use would lead to disciplinary action and/or dismissal.

It is also worth keeping in sharp focus a statement from the DCSF in 2007:

"There are no circumstances that justify adults possessing indecent images of children. Adults who access and possess links to such websites will be viewed as a significant and potential threat to children"

Staff should therefore ensure that they have absolute control of a school mobile device and its use when it is allocated to them. Each member of staff must remember that for a "third party" to use a school mobile device in their home, they would either need to be:

1. Logged on by the member of staff responsible for the mobile device
2. Provided with the confidential log in details by the member of staff responsible for the mobile device

With this in mind, staff should think about who would be culpable in the unlikely event of an allegation being made.

When persons are viewing material on the Internet all people without the assistance of content filters have to make judgements as to whether the content is appropriate or inappropriate. However - inappropriate means different things to different people.

13 Mobile Device Security

All staff should be aware of the need to preserve the confidentiality of certain school information. This is especially true of student and staff "personal information" that is being worked on at school and then taken home to continue that work. All personal information is subject to the Data Protection Act (DPA) and should be treated as such.

For further information relating to the DPA please refer to the "Legal Matters" section.

The layers of security that can protect data on mobile devices are as follows:

- Passwords – staff mobile device must always have passwords and they should not be simple ones. They should include some numbers and/or capitals.
- The passwords should never be left blank. They should also never be set to "standard ones" like "password", "Password", or even "1234". These provide little or no security.
- Passwords must not be stored as part of automatic logon sequences for machines, software or secure websites.
- Staff should ensure that their school mobile device are regularly logged on to the school computer network to ensure their laptops pick up the latest Windows operating system updates from Microsoft and to keep the Microsoft Windows / Microsoft Office license active. These will help prevent the machine being attacked by viruses or "malware.
- Staff pcs do not have a password-protected screensaver set as this tends to interfere with the flow of a lesson. In order to protect data on staff machines, if the computer has to be left unattended, even for a few minutes, users should always press the WIn+L keys to lock their PCs.
- Staff members may only use software licensed by the school, installed by the school's ICT staff. Unauthorised software downloaded from the Internet may compromise the security of the machine and is therefore not permitted.
- Standard memory sticks/portable hard drives may still be used as long as the data they contain is not of a confidential or sensitive nature. If confidential data is lost and it has not been stored on an encrypted medium the member of staff will face disciplinary action. If you are in any doubt, please see a member of the I.T. staff/Business Manager

NB: Please consider the harm that could result from a failure to protect your stored data.

The first four bullet points should be used on all mobile devices regardless of the nature of the data being stored. Any portable storage devices like USB Memory Sticks or portable hard drives should regularly have a scan for viruses.

Clearly, staff shopping lists or weekly timetables require very little security but as soon as either pupil or staff records are being transported then increasing strict security measures need to be utilised.

14 Using Bluetooth

'Bluetooth is an open wireless system that allows you to share files, images, video clips or any other content (appropriate or not) between Bluetooth enabled devices

These devices include many laptops and printers for example but also most mobile phones as well. To protect adults, it is advisable to ensure their Bluetooth is off or 'hidden' on their mobile devices, especially mobile phones, to prevent others from sending content or messages that may be inappropriate or even illegal.

Many adults (and young people) choose "nicknames" for their Bluetooth devices and it is important to choose a nickname that would not be considered inappropriate. The "nickname" is probably inappropriate if you would not want to be addressed by this "nickname" by:

- Your parents

- Your Grandparents
- Your Children
- Work Colleagues
- Any Children with which you might work with.

15 Taking information about students and staff home

Much of the work of teaching staff in particular has, by its very nature, to be performed outside normal school hours and very often at home. This involves taking home reports, attendance records and academic marks. It also includes data accessed remotely, over the Internet, through systems like SIMS and Remote Desktop. In the case of staff in leadership roles the work may include professional reviews or appraisals of other staff. Much of this data that is taken home is classed as personal information in terms of the Data Protection Act 1998 (DPA).

As has been mentioned in the sections on "Laptop security" and "Protecting Data", schools are required to keep this data secure. By this it means that measures have to be put in place that ensure the data cannot fall into the hands of persons who have no right to view it.

- Never leave a computer or laptop logged on under a staff account unattended.
- Do not project student-based information on to a whiteboard/Smartboard.
- Do not leave student-based information visible to students.

Further detail can be found in the section on "Laptop security" and the section on "Protecting Data".

16 Legal Issues

This section aims to illustrate a few of the legal implications of staff working with young people.

16.1 Registration of Staff and Reporting Incidents

16.1.1 What is a DBS Check?

A DBS Check is a Disclosure and Barring Service Check. It has three key purposes:

- Preventing (and keeping records of) unsuitable individuals from working with vulnerable groups
- Check if there's any reason a potential employee is inappropriate for the role that they've applied for
- To respond to referrals from organisations that are concerned that a candidate may not be suitable for a job due to the reasons above

These checks are usually requested by an employer so that they can make safer recruitment decisions.

16.1.2 What types of DBS Check are there?

There are three types of DBS Checks available:

- Basic DBS Checks are the lowest level of DBS Check available – there are no eligibility requirements in place to apply for one and it is not job specific. It will detail any recent, unspent and/or serious convictions
- Standard DBS Checks contain comprehensive criminal record information without a check against the barred list. It will detail spent and unspent convictions, as well as any cautions, warnings or reprimands they have received. This check can only be requested for certain roles – often those in finance or law
- Enhanced DBS Checks are the most comprehensive level of DBS Check available, detailing spent and unspent convictions as well as the ability to check against the child or adults barred list. Police authorities may also disclose any additional relevant information. This level of check is only available in specific roles, typically those involving regulated activity with children or vulnerable adults

16.1.3 What jobs require a DBS Check?

As mentioned above certain roles will require applicants to have a valid DBS Check certificate. Enhanced DBS Checks are necessary in any workplace where employees (or volunteers) are likely to engage in regulated activity with children or vulnerable people. These include:

- Schools
- Children's homes
- Hospitals
- Care homes

Additionally, DBS Checks are required for employees that handle certain sensitive data, such as employees with access to fostering or adoption records

16.1.4 How can I get a DBS Check?

If an organisation requires employees or volunteers to have a Standard or Enhanced DBS Check they must apply on their behalf. If a Basic DBS check is required, this can either be obtained by the employer or the applicant.

Self-employed workers who require a Standard or Enhanced DBS Check should ask the organisation they're working for to apply on their behalf.

16.1.4.1 Why do I need a DBS Check? – Conclusion

DBS Checks are a vital part of safeguarding for an organisation, as well as ensuring that they are able to employ suitable candidates. While applying for a DBS Check can be a confusing process, it is important to consider DBS Checks if you're in an industry such as teaching or medicine.

16.2 Inappropriate and Illegal Material/Content

Some types of Internet material or content are considered inappropriate for staff to be accessing. It is a criminal offence to access/create/save some types of information from the Internet.

Clearly all staff should not view, download or create inappropriate, illegal or criminal content. Any member of staff that does so should be aware that the sanctions that can be applied range from disciplinary to criminal. Access to the Internet in schools is always logged and can be monitored or retrospectively investigated.

As a result, staff should be alert to the possibility of accessing inappropriate and illegal material and take steps to avoid this. Staff should avoid creating material that could result in civil or criminal action.

- Any activity that is illegal would be a breach of civil law and could result in, upon conviction, having to pay damages / compensation to an individual or organization that brought a case to court.
- Any activity that is a criminal offence, if proven in court, would lead to a criminal record and possible fines or imprisonment.

The range of behaviours is clearly huge and cannot possibly be covered completely in this guidance but some could be so serious as to constitute gross misconduct. Examples of inappropriate behaviour include but are not limited to:

- Posting on social networking sites offensive or insulting comments about the school or its staff. (This could be illegal if it is defamatory and/or a malicious falsehood resulting in civil action)
- Attempting to access adult pornography of any type using the school internet or on school computers.
- Making indecent, offensive or threatening comments about pupils or colleagues on social networking sites (Potentially a criminal offence under Protection from Harassment Act 1997)
- Contacting pupils by email or social networking without prior senior management approval.
- Trading in sexual aids, fetish equipment or adult pornography.

Although all these activities are unacceptable and may well lead to disciplinary action, they are not all illegal or criminal. However, possessing or distributing indecent images of a person under 18 is a criminal offence.

Even viewing such images on-line may well constitute possession even if not saved. Saving such images on a computer is classed as “creating” those images.
The police have a system of grades for different types of indecent image although defining whether images are regarded as indecent would ultimately be down to a jury to decide.

All staff should be aware that in the case of any material that is illegal/criminal to possess, an investigation might lead to: criminal investigation, prosecution, dismissal and barring. The possession of material that is inappropriate, but legal can still lead to disciplinary action, dismissal and barring even if there is no criminal prosecution. It is well worth remembering that children may be harmed or coerced into posing for such images and are, therefore, victims of child sexual abuse.

It is important to note that the school force both staff and students use ‘Strict safe search’ when using search engines like Google and Bing this can reduce the risk of inadvertent access to inappropriate or illegal sites.

This greatly reduces the risk of inappropriate or indeed illegal images appearing as a result of quite innocent search queries. Internet access within school is protected by the school’s own Lightspeed filter. Although these systems cannot guarantee the safety of staff and pupils, they go a long way to reducing the likelihood of users accessing inappropriate material. If you become aware of an

inappropriate site, please report it immediately to the Network Manager or member of SLT, so that the site can be added to a stored list of 'banned sites' and/or reported the IT department.

16.3 Protecting Data

Any information that can be identified as relating to a named, living individual such as: name, age, sex, attendance records, assessment marks etc is classed as "personal information".
Whether in an electronic form saved on a laptop, on a peripheral device (such as a "USB Memory stick") or even in paper form - the Data Protection Act 1998 (DPA) requires that personal data is kept secure by the school and therefore by all staff.

The measures to keep the data secure must apply whether the data is held in school, in transit, or at home. Schools and their employees are required by the act to take appropriate measures to keep personal data secure. These measures will be both organisational and technical. The extent of these measures needs to reflect the harm that would result from a failure to protect it.

Staff should consider not storing information at all unless it is for school related purposes and securely deleting files after use. If it is necessary to hold the information then all staff should ensure that it is not available to people that have no need or indeed right to handle it within the establishment.

For those members of staff that need to have access to confidential data the safest long-term storage location must be the school network, which has a remote backup facility.

The storage of data on laptop hard disks/USB Portable hard drive/USB Memory sticks and transfer by e-mail to unsecure email addresses or other means is not acceptable practice. This is due to risks including mislaying a USB Portable Hard

Drive/ USB Memory Stick and/or laptop theft enabling a third party to access confidential data. stick and laptop theft from a vehicle are common events. The loss of "memory sticks" is particularly common.

Schools can apply a number of methods to keep data secure, which can be applied in layers depending on the risks involved. These "layers" are described in the section on the "Use of laptops".

All staff are strongly advised to ensure that they have read and understand the school policy regarding data protection. To lose control of personal data while not complying with the school policy would be difficult to defend and may lead to disciplinary action and/or personal prosecution.
Any company or institution who keeps your personal information on file – electronically or in hard copy format – must ensure that they adhere to the rules as laid down by the Data Protection Act. Failure to do so could lead to prosecution, a compensation pay-out and also a hefty fine. As a company or public sector institution the following must be carried out under the Act:

- All information must be used only for the purposes it is intended for
- Any personal information must not be passed to a third party without prior consent
- All personal information must be kept strictly for the recommended period of time only ● Companies or institutions must supply copies of all information kept to the individual involved within a set time scale upon request

As mentioned previously a failure to adhere to these rules can lead to a prosecution which can also put the company at risk of losing their ability to store information on private individuals. This in itself can be very damaging to a company's ability to trade.

16.4 Offences Relating to Staff Communications

There are a number of laws in the UK that can relate to communications passing on hate, harm or harassment.

All staff should be cautious when composing any communication via in an electronic format. It is all too easy to be thinking one thing when you are typing and yet, when it is seen, out of the context of that thought process; appear to be saying something totally different. That difference can manifest itself as being offensive, indecent or even a threat when read by the recipient.

It is an offence to send an indecent, offensive or threatening message with the intention of causing the "victim" distress or anxiety. This applies if the message is on paper or using technology including through e-mail, Instant Messaging or social networking sites.

Charges can be based on the Malicious Communications Act 1998 or the Protection from Harassment Act 1997. Cases where messages are conveyed by phone can also be an offence under the Telecommunications Act 1984.

If the e-mails, or other messages are shown to be racist or motivated by religious hostility then charges could be brought of Racially or Religiously Aggravated Harassment contrary to of the Crime and Disorder Act 1998.

Staff should think a second time before you "click on send" and if you have any doubts about how it might look or how it may be interpreted, then don't send it.

17 Summary

In conclusion, as was stated at the start of this document, there can be no rigid set of rules of Do's and Don'ts to govern all of these complex issues.

Below is a list some of the things that staff should do as well as some that they should not do – at least, not without a considerable degree of transparency as well as the knowledge of the school Senior Management Team (SLT). In some cases, this should include the written consent of SLT. Some of these are listed in the table below and any reference to Facebook extends to all other social networking sites.

Things staff should do	Things staff should not do
• Staff passwords for Internet based accounts such as Facebook should always be of at least eight characters including some numbers and or capitals. Restrict Facebook information such as: profiles, photos, videos and postings to their "friends" only. • Use passwords for laptops – these should include some numbers and or capitals. • Do not give your passwords for any device or any website to anyone else. • Do not leave passwords on a "post-it" in full view of passers-by. • Set mobile phones so that Bluetooth is either off or 'hidden'. Do check out websites, in school, before using them with a class. • Do make sure that if you are asked to monitor or investigate the Internet activity of staff or pupils that you have the written backing of the school SLT to do so. • Follow the school policy on keeping personal information that you need to take away from home secure.	• Give personal e-mail addresses to young people. Give personal mobile numbers to young people. Give their home telephone number to young people. • Accept students as "friends" on a personal Facebook account. • Use a personal camera or camcorder to record images of children. • Use personal computer equipment to process images of students at home. • Form contact with students beyond your professional duties and beyond "normal working hours" for your role. • Behave inappropriately on the Internet. Examples of this can be found in the "Inappropriate and Illegal Material/Content" section.

18 Glossary

18.1.1 Personal Information

"Personal information" (as referred to in the Data Protection Act). means information that relates to a living individual who can be identified from that information, or from other information, which is the possession of the school. It also includes any expression of opinion about the individual as in school reports or professional appraisals).

18.1.2 Bluetooth

An open wireless system that allows you to share files, images, video clips or audio streams between Bluetooth enabled devices. These devices include many laptops, printers, scanners, and headsets but also most mobile phones as well.

18.1.3 Unified Sign On (USO) also known as Single Sign On (SSO)

USO - A single username and password for every relevant student and member of staff in West Sussex state-maintained schools, granting access to all supported resources on the schools' network.

18.1.4 USB Memory Stick/Flash Drive/Pen Drives

A USB flash drives are data storage devices that have largely replaced "Floppy disks" as a method of transferring data. They consist of a memory chip attached to a USB plug and encased in plastic. They

are rewritable in the same way as “floppies” but with a vastly high capacity ranging up to many gigabytes.

18.1.5 Social network Sites

Social network Sites focus on building and reflecting social network or social relationship among people who share interests and/or activities. Users can share what they are doing/thinking together with photos, videos or web-links with people they have accepted as “friends” on their chosen site. Social Networking Sites includes sites such as Facebook, TikTok, Twitter (X), Instagram and LinkedIn.
DCSF – the Department for Children, Schools and Families (replaced the DfES – the Department for Education and Schools).

18.1.6 File-shredding software

This software removes files from your hard drive or USB memory stick without fear they could be recovered. It does this by rewriting the files with random series of binary data multiple times. This process is often called shredding. One open source (free) example of this software is one called “File shredder” but there are many others that could just as easily be used.
Memory cards – is memory that is encased in various sizes and shape of plastic that are commonly used in digital cameras and camcorders. Examples include: SD, CF, XD and MS cards.

18.1.7 Malware

Malware: short for *malicious software* is software designed to infiltrate a computer system without the owner's consent. It includes: computer viruses, worms, trojans, most rootkits, spyware, dishonest adware, crimeware and other malicious and unwanted software. It is often transmitted via e-mails, social networking sites or malicious websites. The expression is a general term used to mean a variety of forms of hostile, intrusive, or just annoying software or program code.

18.1.8 Secure

Various ways of storing or transmitting information are considered to be “secure” if they are encrypted (scrambled) so that other, unauthorised people cannot view that information. This data could be in any number of places including but not limited to:

- Held on a website.
- Transmitted to or from a website
- Stored on a USB Flash Drive.
- Stored on a laptop hard disk.

18.1.9 POVA – The Protection of Vulnerable Adults scheme. POCA

The Protection of Vulnerable Children Act.

19 Appendix

20 Worthing High School

Staff User Agreement Form for use of School Network and Related Internet Resources

As a user of the School Network, I agree to follow the policy for Networks and Internet Resources. I will use the network in a responsible way and observe all the restrictions explained in the school acceptable use policy. I agree to report any misuse of the network and/or ICT equipment to the IT Manager.

If I do not follow the policy, I understand that this may result in loss of access, security privileges and/or disciplinary proceedings.

I understand that I am responsible for my email address and may be held accountable for any inappropriate mail sent from my email address.

I understand that I am required to read the school's policy document entitled 'Guidance for the Safer Use of the Internet by Staff Working with Young People'

Staff Name: _____

Staff Signature: _____

Date:

Please detach this form from the Booklet & return to the Office Manager.

Thank you.

21 Guidance for the Safer Use of the Internet and social media by Staff Working with Young People

21.1 Introduction

In addition to a school's educational responsibility, the safe use of the Internet in a school setting involves further responsibilities in terms of the protection of children and vulnerable adults as well as Health and Safety.

All adults working with children and young people are clearly in a position of trust and as such they must understand the responsibilities that their work place them under. Adults in this area of work need to ensure they are: competent, confident and safe when working with new technology, especially when connected to the Internet.

Employers have a duty of care towards their employees under the Health and Safety at Work Act 1974[1]. This duty requires them to provide a safe working environment for staff and guidance about safe working practices.

This same act also imposes a duty on employees [2] to take care of themselves and anyone else that may be affected by their actions or failings. An employer's duty of care to their staff and the staffs' duty of care towards children should not conflict. The following can fulfil these 'duties':

- The production of these guidelines
- The promotion of these guidelines by schools
- These guidelines being adopted and followed by employees.

This guidance sets out to identify some examples of appropriate and safer types of behaviour for adults working in a school context. For the purposes of this guide the term "staff" includes any adults that are working with children: teachers, teaching assistants and other helpers both paid and unpaid.

There can be no rigid set of rules to govern such complex issues. A constant stream of new technologies and practices in the use of the Internet and those technologies that use it mean that it is nearly impossible to include all possible scenarios at any one time let alone the future.

We hope that a blend of examples and advice will help build a feel for what the dangers are in using the Internet as well as the consequences of inappropriate use: WSCC ICT in Schools Team – June 2013

21.2 The Aims of this Guide

For the purposes of this guide the term "staff" includes any adults that are working with children: teachers, teaching assistants and other helpers both paid and unpaid.

Although this guide is not a contractual requirement, nor is it legally binding, it does aim to help staff with the following:

- To help adults that work with children to do so safely and responsibly with the Internet and associated technologies.
- To clarify which behaviours, constitute safe practice and which types of behaviour should be avoided by staff.
- To help staff, in conjunction with: School Acceptable Use Policies, Filter Policies, Network monitoring software and School laptop agreements, to understand the boundaries of acceptable behaviour.
- To mitigate the risk of having malicious or just misplaced allegations being made against staff.
- To support school managers and leaders in establishing: policies, codes of behaviour and a workplace ethos that safeguards staff as well as young people in their organisation.
- To assist school management teams in giving a clear message that unsafe or, even more so unlawful behaviour is unacceptable and that where appropriate, disciplinary or legal action will be taken.

21.3 Using this Guidance

This guide is intended to support staff in their use of the Internet whilst bearing in mind their professional responsibilities.

It is intended that staff reduce the risk of inadvertently behaving in an inappropriate or illegal fashion when using the Internet by reading and following the advice given in this guidance.

The guidance is also intended to reduce the risk of unfounded allegations of inappropriate behaviour without unnecessarily restricting the free use of the Internet.

21.3.1 Staff

In order to maximise the potential of these guidelines for staff themselves the following is suggested:

- If in doubt about your use of the Internet and whether it is acceptable you should consult this document to see if that specific example is covered directly.
- If in doubt about whether your use of the Internet, and this document does not cover that example directly – consult the school leadership and school policies to ensure that your actions are both transparent and endorsed by the school leadership team.
- Always consider how any action on the Internet would look to a third party out of that particular context and target audience. This is particularly true of photographs and comments linked to “in jokes” that to a third party may appear inappropriate at best.
- Only publish material on the Internet that you would be happy to share with parents, pupils and both present and future employers/employees/colleagues.
- Keep this document –alongside other policy documents to guide their actions when using Internet technologies.

21.4 Contact with Children Outside of School Hours

Increasingly staff and students alike are encouraged to personalise learning with the use of technologies and contact extending beyond the traditional classroom. This contact often involves the use of e-mail as well as.

Although there are undoubted educational benefits for the use of these technologies in order to encourage collaboration and individual research there are "risks" in not doing so safely.

The DCSF stated in 2007 that:

"Communication between adults and children, by whatever method, should take place within clear and explicit professional boundaries. Adults should not share any personal information with the child or young person. They should not request, or respond to, any personal information from the child / young person, other than that which might be appropriate as part of their professional role. Adults should ensure that all communications are transparent and open to scrutiny."

Staff should limit contact with young people to official channels of communication such as school-based e-mail accounts such as the school "worthinghigh.net" accounts. Staff should not give their personal (as opposed to "work") e-mail addresses to young people to allow access outside of school hours.

Staff should also take great care in the use of nicknames or automatic signatures. As an example, "Sexylegs" is not an appropriate signature for either a pupil or member of staff when in an education setting.

In terms of exchanges on forums and (even more so) chat rooms they should be limited to school based, open, transparent and logged locations. School senior managers may wish to incorporate this recommendation into an e Safety policy.

"Public" sites such as: Google mail (Gmail), Hotmail and others offering free e-mail accounts, Instant Messaging (IM) and Forums should be avoided by staff for communications with students. Although these services are openly available and quite acceptable between adult friends, they cross the "clear and explicit professional boundaries" that are offered by school based professional channels.

The DCSF stated in 2007 that:

"Adults should be circumspect in their communications with children and young people so as to avoid any possible misinterpretation of their motives or any behaviour which could be construed as grooming."

Staff should not use their private mobile phones as a method of communication with students at any time without specific consent and knowledge of the school senior leadership team. This includes giving their personal home or mobile phone numbers to pupils to allow those pupils to contact them. Even then this contact should be for only clearly defined purposes agreed by senior management.

21.5 Social Networking Sites

Social networking is a way of life for most young people and many adults. However, staff working with children and young people should review their use of social networks in the light of their professional responsibilities. What may have been acceptable as a university student may not be acceptable when working with young people.

If a member of staff were to use this type of communication with students, some consideration should be given as to how it might appear to a parent or an officer investigating any complaint. Compared with a conversation in a classroom the use of these technologies inevitably increases the risk exchanges being seen out of context or misinterpreted.

If any social networking site is to be used with pupils, schools should set up a totally separate account for this purpose. Naturally this should be done with the full agreement of, and visibility to the senior management of the school concerned.

Staff communicating with students online must have an environment that is both transparent and under their control. An essential first requirement is that staff should know with whom they are talking online.

Currently very few public social networking sites authenticate their users as they tend to use automated registration systems that provide only very limited checks. Existing rules with these sites set lower limits according to user's ages. Although this is not strictly enforced it may prove a barrier to some activities.

For the purposes of this guide, we are going to use Facebook as an example of "Social Networking Sites" but the same principles apply to other similar sites such as Instagram, TikTok, X (formerly Twitter), Snapchat etc.

21.6 Who Are Your Facebook Friends?

In Internet parlance the term "friends" can mean almost anything. This ranges from your best, lifelong real-life friend to someone you have never met in your life. Perhaps someone who happens to be a friend of somebody else that knows someone you actually know in person. In extreme cases, a friend invite may come from a person who is claiming (on the Internet) to be someone totally different that you do actually know but is in fact a malicious user seeking to cause mischief and or harm/distress.

Although some people like trying to collect as many "friends" as they can as a "status symbol" staff should be very wary of accepting people as Facebook friends that they don't know personally and can verify that they are who they say they are.

Sometimes a person claiming to be one person on the Internet is in reality someone totally different. Much of the security of Social Networking sites like Facebook relies on allowing only friends to see certain material. Photographs are an example of this. If you don't have control of who your "friends" are you don't have control of your information.

Staff would be ill advised to accept students as "friends" on Facebook. The risks of even perfectly innocent exchanges being misinterpreted from this kind of contact are quite real and members of staff doing so are also leaving themselves exposed to an unnecessary risk of allegations of misconduct.

Once a person can see any information about you whether it is a comment, a photo or a video, they can capture it and do whatever they like with it on the Internet. This can include the images being manipulated to depict something quite different from the original. This can sometimes go badly wrong for the original owner of the images.

21.7 Privacy Settings – Profile on Facebook

Under Settings/Privacy Settings you can control who can see various aspects of your Facebook pages. You can allow everyone on the Internet to see things like: your personal information (including contact information), work information etc. You can however restrict access to only your "Friends".

It is strongly recommended that staff restrict this kind of information to their "friends" only. The same applies to photos, videos and postings made by the individuals concerned.
You might share your address, phone number, personal photographs with your friends in real life but you wouldn't stick copies of them together with photographs of yourself on a bus station notice board – so why do the same on the Internet?

21.8 Social Networking Site Security

Staff should be very careful with their password information – just like the passwords for their network login or their bank card PIN number. They should not be shared with anyone at any time and yes, this does include a "post it" stuck on your desk/monitor!

Passwords should also be complex and not easily "guessable". They should consist of a combination of at least 8 characters/numbers/symbols.

The concept of "Facebook Rape" sounds strange but it involves a second party gaining access to login details for Facebook and using that access to:

- Send unpleasant messages to third parties using your identity
- Post unpleasant material on the Internet under your name
- Post photos or videos that could be distressing to the victim or their true friends but under the name of the victim

In all of these cases the unpleasant material would look as if the victim had produced it. Needless to say, this can be very, very distressing for the victim concerned.

It is well known that the spread of malware and viruses through social networking sites is prevalent. This is due to the nature of the openness and the large degree of interaction that is encouraged within these environments. This is their strength but, in this context unfortunately, their weakness as well.

Whilst Anti-Virus software should be installed on all school laptops, it cannot be guaranteed to offer total protection. It is therefore strongly recommended that no third-party applications or software are downloaded from the Internet on to school laptops. The restriction on downloading and executing software forms the best defence mechanism from malicious attack through viruses and Malware.

21.9 Using Social Networking Sites

You shouldn't say or show anything online that you wouldn't want the following people to know about:

- Your parents
- Your Children
- Work Colleagues
- Any employer or prospective employer now, or in the future.
- Any Children with which you might work with.

Posting amusing remarks about their school, colleagues or students only to find them republished elsewhere by “friends”, has caught out some adults. Even innocent remarks, taken out of context, could be misinterpreted (unintentionally or otherwise) and posted elsewhere by a “friend”.