Brentford School for Girls

E-Safety Policy 2015

Contents

1. Introduction and Overview

Rationale

The purpose of this policy is to:

- set out the key principles expected of all members of the school community at Brentford School for Girls with respect to the use of ICT-based technologies
- safeguard and protect the children and staff of Brentford School for Girls
- assist school staff working with children to work safely and responsibly with the internet and other communication technologies and to monitor their own standards and practice
- set clear expectations of behaviour and/or codes of practice relevant to responsible use of the internet for educational, personal or recreational use
- have clear structures to deal with online abuse such as cyberbullying which are cross referenced with other school policies
- ensure that all members of the school community are aware that unlawful or unsafe behaviour is unacceptable and that, where appropriate, disciplinary or legal action will be taken
- minimise the risk of misplaced or malicious allegations made against adults who work with students

The main areas of risk for our school community can be summarised as follows:

Content

- exposure to inappropriate content, including online pornography, ignoring age ratings in games (exposure to violence associated with often racist language), substance abuse
- lifestyle websites, for example pro-anorexia/self-harm/suicide sites
- hate sites
- content validation: how to check authenticity and accuracy of online content

Contact

- grooming
- cyber-bullying in all forms
- identity theft (including 'frape' (hacking Facebook profiles)) and sharing passwords

Conduct

- privacy issues, including disclosure of personal information
- digital footprint and online reputation
- health and well-being (amount of time spent online (internet or gaming))
- sexting (sending and receiving of personally intimate images) also referred to as SGII (self generated indecent images)

copyright (little care or consideration for intellectual property and ownership – such as music and film)

(Ref Ofsted 2013)

Scope

This policy applies to all members of Brentford School for Girls community (including staff, students / pupils, volunteers, parents / carers, visitors, community users) who have access to and are users of academy ICT systems, both in and out of Brentford School for Girls.

The Education and Inspections Act 2006 empowers Headteachers to such extent as is reasonable, to regulate the behaviour of students / pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, or other e-safety

incidents covered by this policy, which may take place outside of the school, but is linked to membership of the school. The 2011 Education Act increased these powers with regard to the searching for and use of electronic devices and the deletion of data. In the case of both acts, action can only be taken over issues covered by the published Behaviour Policy.

Brentford School for Girls will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents / carers of incidents of inappropriate e-safety behaviour that take place out of school.

Role	Key Responsibilities
Headteacher	• To take overall responsibility for e-Safety provision • To take overall responsibility for data and data security • To ensure the school uses an approved, filtered Internet Service, which complies with current statutory requirements • To be responsible for ensuring that staff receive suitable training to carry out their e-safety roles and to train other colleagues, as relevant • To be aware of procedures to be followed in the event of a serious e-Safety incident. • To receive regular monitoring reports from the Safeguarding Co-ordinator • To ensure that there is a system in place to monitor and support staff who carry out internal e-safety procedures (e.g. network manager)

Safeguarding Co-ordinator / Designated Child Protection Lead	• To take day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies / documents
	• To promote an awareness and commitment to e-safeguarding throughout the school community
	• To ensure that e-safety education is embedded across the curriculum
	• To liaise with school ICT technical staff
	• To communicate regularly with SLT and the designated e-Safety Governor / committee to discuss current issues, review incident logs and filtering / change control logs
	• To ensure that all staff are aware of the procedures that need to be followed in the event of an e-Safety incident
	• To ensure that an e-Safety incident log is kept up to date
	• To facilitate training and advice for all staff
	• To liaise with the Local Authority and relevant agencies
	• Is regularly updated in e-safety issues and legislation, and be aware of the potential for serious child protection issues to arise from:
	  • sharing of personal data
	  • access to illegal / inappropriate materials
	  • inappropriate on-line contact with adults / strangers
	  • potential or actual incidents of grooming
	  • cyber-bullying and use of social media

Governors / E-safety governor	• To ensure that the school follows all current e-Safety advice to keep the children and staff safe • To approve the E-Safety Policy and review the effectiveness of the policy. A member of the Governing Body has taken on the role of E-Safety Governor • To support the school in encouraging parents and the wider community to

Role	Key Responsibilities
	become engaged in e-safety activities • The role of the E-Safety Governor will include: • regular review with the Safeguarding Co-ordinator
ICT head of department	• To oversee the delivery of the e-safety element of the Computing curriculum • To liaise with the safeguarding coordinator where necessary
Network Manager	• To report any e-Safety related issues that arises, to the safeguarding coordinator. • To ensure that users may only access the school's networks through an authorised and properly enforced password protection policy, in which passwords are regularly changed • To ensure that provision exists for misuse detection and malicious attack e.g. keeping virus protection up to date) • To ensure the security of the school ICT system • To ensure that access controls / encryption exist to protect personal and sensitive information held on school-owned devices • To ensure the school's policy on web filtering is applied and updated on a regular basis • To keep up to date with the school's e-safety policy and technical information in order to effectively carry out their e-safety role and to inform and update others as relevant • To ensure that the use of the school's ICT infrastructure (*network / SIMS / Virtual Learning Environment / remote access / email*) is regularly monitored in order that any misuse / attempted misuse can be reported to the safeguarding coordinator and / or Headteacher for investigation and action. • To ensure appropriate backup procedures exist so that critical information and systems can be recovered in the event of a disaster • To keep up-to-date documentation of the school's e-security and technical procedures • Oversight of the finger printing / access to cashless payment scheme • To ensure that all data held on pupils on FROG is adequately protected
Virtual Learning Platform Leader	• To work with the Network Manager to ensure that all data held on pupils on FROG is adequately protected
Data Manager/admin staff	• To ensure that all data held on pupils on the school office machines have appropriate access controls in place
Teachers	• To embed e-safety issues in all aspects of the curriculum and other school activities • To supervise and guide pupils carefully when engaged in learning activities involving online technology (including, extra curricular and extended school activities if relevant) • To ensure that pupils are fully aware of research skills and are fully aware of legal issues relating to electronic content such as copyright laws

Role	Key Responsibilities
All staff	• To read, understand and help promote the school's e-Safety policies and guidance • To read, understand, sign and adhere to the school staff Acceptable Use Agreement / Policy • To be aware of e-safety issues related to the use of mobile phones, cameras and hand held devices and that they monitor their use and implement current school policies with regard to these devices • To report any suspected misuse or problem to the safeguarding coordinator • To maintain an awareness of current e-Safety issues and guidance e.g. through CPD • To model safe, responsible and professional behaviours in their own use of technology • To ensure that any digital communications with pupils should be on a professional level and only through school based systems, never through personal mechanisms, e.g. email, text, mobile phones etc.
Pupils	• Read, understand, sign and adhere to the Student / Pupil Acceptable Use Policy • Have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations • To understand the importance of reporting abuse, misuse or access to inappropriate materials • To know what action to take if they or someone they know feels worried or vulnerable when using online technology • To know and understand school policy on the use of mobile phones, digital cameras and hand held devices • To know and understand school policy on the taking / use of images and on cyber-bullying • To understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that the school's E-Safety Policy covers their actions out of school, if related to their membership of the school • To take responsibility for learning about the benefits and risks of using the internet and other technologies safely both in school and at home • To help the school in the creation/ review of e-safety policies
Parents/carers	• To support the school in promoting e-safety and endorse the Parents' Acceptable Use Agreement which includes the pupils' use of the internet and the school's use of photographic and video images • To read, understand and promote the school Pupil Acceptable Use Agreement with their children • To access the school website / on-line student records in accordance with the relevant school Acceptable Use Agreement. • To consult with the school if they have any concerns about their children's use of technology

Role	Key Responsibilities
External groups	• Any external individual / organisation will sign an Acceptable Use Policy prior to using any equipment or the internet within school

Communication:
The policy will be communicated to staff/pupils/community in the following ways:

- Policy to be posted on the school website
- Policy to be part of school induction pack for new staff
- Acceptable use agreements to be issued to and signed by both staff and students, usually on entry to the school
- Acceptable use agreements to be held in pupil and personnel files
- Acceptable use agreements highlighted to all pupils at the start of each year

Handling complaints:

- The school will take all reasonable precautions to ensure e-Safety. However, owing to the international scale and linked nature of Internet content, the availability of mobile technologies and speed of change, it is not possible to guarantee that unsuitable material will never appear on a school computer or mobile device. Neither the school nor the Local Authority can accept liability for material accessed, or any consequences of Internet access.

- Staff and pupils are given information about infringements in use and possible sanctions. Sanctions available include:
  - interview/counselling by tutor / Head of Year / Safeguarding Coordinator / Headteacher
  - informing parents or carers
  - removal of Internet or computer access for a period, [which could ultimately prevent access to files held on the system, including examination coursework]
  - referral to LA / Police

- Our Safeguarding Coordinator acts as first point of contact for any complaint. Any complaint about staff misuse is referred to the Headteacher

- Complaints of cyberbullying are dealt with in accordance with our Anti-Bullying Policy. Complaints related to child protection are dealt with in accordance with school / LA child protection procedures

2. Education and Curriculum

Pupil e-Safety curriculum

This school

- Has a clear, progressive e-safety education programme as part of the Computing curriculum / PSHCE curriculum there is some coverage of relevant issues in the KS3 ICT curriculum in year 8 and 9 and in PSHCE across the school. It covers a range of skills and behaviours appropriate to a student's age and experience, including:

- to STOP and THINK before they CLICK
- to develop a range of strategies to evaluate and verify information before accepting its accuracy
- to be aware that the author of a web site / page may have a particular bias or purpose and to develop skills to recognise what that may be
- to know how to narrow down or refine a search
- to understand how search engines work and to understand that this affects the results they see at the top of the listings
- to understand acceptable behaviour when using an online environment / email, i.e. be polite, not to use bad or abusive language or other inappropriate behaviour, keeping personal information private
- to understand how photographs can be manipulated and how web content can attract the wrong sort of attention
- to understand why on-line 'friends' may not be who they say they are and to understand why they should be careful in online environments;
- to understand why they should not post or share detailed accounts of their personal lives, contact information, daily routines, location, photographs and videos and to know how to ensure they have turned-on privacy settings
- to understand why they must not post pictures or videos of others without their permission;
- to know not to download any files, such as music files, without permission
- to have strategies for dealing with receipt of inappropriate materials
- to understand why and how some people will 'groom' young people for sexual reasons
- to understand the impact of cyberbullying, sexting and trolling and know how to seek help if they are affected by any form of online bullying
- to know how to report any abuse including cyberbullying, and how to seek help if they experience problems when using the internet and related technologies, i.e. parent or carer, teacher or trusted staff member, or an organisation such as Childline or the CLICK CEOP button

- Plans internet use carefully to ensure that it is age-appropriate and supports the learning objectives for specific curriculum areas
- Will remind students about their responsibilities through an Acceptable Use Policy which every student will sign on entry to the school
- Will automatically remind users of this agreement when they log on to the school network.
- Ensures staff will model safe and responsible behaviour in their own use of technology during lessons.
- Ensures that when copying materials from the web, staff and pupils understand issues around plagiarism; how to check copyright and also know that they must respect and acknowledge copyright / intellectual property rights
- Ensures that staff and pupils understand the issues around aspects of the commercial use of the internet, as age appropriate. This may include risks such as pop-ups, buying on-line and on-line gaming / gambling.

Staff and governor training

This school

- Provides staff with information on how to send or receive sensitive and personal data and understands the requirement to encrypt data where the sensitivity requires data protection
- Makes training available to staff on e-safety issues as required
- Keeps staff updated on e-safety issues and the school's e-safety education program through annual updates
- Provides, as part of the induction process, all new staff, including those on placement and work experience, with information and guidance on the e-Safeguarding policy and the school's Acceptable Use Policies.

Parent awareness and training

This school

- Runs a rolling programme of advice, guidance and training for parents, including:
    - the introduction of the Acceptable Use Agreements to new parents, to ensure that principles of e-safe behaviour are made clear
    - useful advice in information leaflets, school newsletters and on the school web site
    - suggestions for safe Internet use at home
    - provision of information about national support sites for parents

3. Expected Conduct and Incident management

Expected conduct

In this school, all users:

- are responsible for using the school ICT systems in accordance with the relevant Acceptable Use Policy which they will be expected to sign before being given access to school systems
- understand the importance of misuse or access to inappropriate materials and are aware of the consequences
- understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that the school's E-Safety Policy covers their actions out of school, if related to their membership of the school
- will be expected to know and understand school policies on the use of mobile phones, digital cameras and hand held devices. They should also know and understand school policies on the taking / use of images and on cyber-bullying

Staff

- are responsible for reading the school's e-safety policy and using the school ICT systems accordingly, including the use of mobile phones, and hand held devices

Students

- should have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations

Parents/Carers

- should provide consent for pupils to use the internet, as well as other technologies, as part of the e-safety acceptable use agreement form at time of their child's entry to the school
- should know and understand what the 'rules of appropriate use' are and what sanctions result from misuse

Incident Management

In this school:

- there is strict monitoring and application of the e-safety policy and a differentiated and appropriate range of sanctions, though the attitudes and behaviour of users are generally positive and there is rarely need to apply sanctions
- all members and its wider community are encouraged to be vigilant in reporting issues, in the confidence that issues will be dealt with quickly and sensitively, through the school's escalation processes.
- support is actively sought from other agencies in dealing with e-safety issues
- parents / carers are specifically informed of e-safety incidents involving young people for whom they are responsible
- We will contact the police if one of our staff or pupils receives online communication that we consider is particularly disturbing or breaks the law

How will infringements be handled?

Whenever a student or staff member infringes the e-Safety Policy, the final decision on the level of sanction will be at the discretion of the school management. Please see Appendices 5 and 6 for guidance.

4. Managing the ICT infrastructure

- **Internet access, security (virus protection) and filtering**

This school:

- Has the educational filtered secure broadband connectivity via its current ISP and in-house UTM.
- Uses an appropriate filtering system which blocks sites that fall into categories such as pornography, race hatred, gaming, sites of an illegal nature, etc. All changes to the filtering policy are logged and only available to staff with the approved 'web filtering management' status
- Uses user-level filtering where relevant, thereby closing down or opening up options appropriate to the age / stage of the students
- Ensures network health through use of anti-virus software etc. and network set-up so staff and pupils cannot download executable files
- Uses an approved system of secured email to send personal data over the internet and uses encrypted devices or secure remote access where staff need to access personal level data off-site
- Blocks all chat rooms and social networking sites except those that are part of an educational network or approved Learning Platform
- Only unblocks other external social networking sites for specific purposes
- Has blocked pupil access to music download or shopping sites – except those approved for educational purposes
- Uses security time-outs on internet access where practicable / useful
- Works in partnership with the ISP / UTM manufacturers to ensure any concerns about the system are communicated so that systems remain robust and protect students;
- Is vigilant in its supervision of pupils' use at all times, as far as is reasonable
- Ensures all staff and students have signed an acceptable use agreement form and understands that they must report any concerns
- Ensures pupils only publish within an appropriately secure environment
- Requires staff to preview websites before use [where not previously viewed or cached] and encourages use of the school's Learning Platform as a key way to direct students to age / subject appropriate web sites;
- Plans the curriculum context for internet use to match pupils' ability, using child-friendly search engines where more open Internet searching is required eg yahoo for kids or ask for kids , Google Safe Search etc.
- Is vigilant when conducting 'raw' image search with pupils e.g. Google image search
- Informs all users that internet use is monitored
- Informs staff and students that that they must report any failure of the filtering systems directly to the Network Manager / ICT Support Team
- Makes clear all users know and understand what the 'rules of appropriate use' are and what sanctions result from misuse, through staff meetings and teaching programme
- Provides advice and information on reporting offensive materials, abuse/ bullying etc available for pupils, staff and parents
- Immediately refers any material that may be illegal to the appropriate authorities, such as the police

- **Network management (user access, backup)**

This school

- Uses individual, audited log-ins for all users
- Uses guest accounts for external or short term visitors for temporary access to appropriate services
- Uses teacher 'remote' management control tools for controlling workstations / viewing users / setting-up applications and Internet web sites, in the computer suites
- Has additional local network auditing software installed
- Ensures the Network Manager is up-to-date with relevant services
- Stores all data within the school in a manner that conforms to the UK data protection requirements.For pupils and staff using mobile technology and where the storage of data is online, this will conform to the EU data protection directive where storage is hosted within the EU

To ensure the network is used safely, this school:

- Ensures staff read and sign that they have understood the school's e-safety Policy. Following this, they are set-up with Internet, email access and network access. Online access to service is through a unique, audited username and password. We also use the same username and password for access to our school's network
- Controls staff access to the schools' management information system via an integrated login
- Ensures all pupils have their own unique username and password which gives them access to the internet, the Learning Platform and their own school approved email account
- Makes clear that no one should log on as another user and makes clear that pupils should never be allowed to log-on or use teacher and staff logins as these have far less security restrictions and inappropriate use could damage files or the network
- Has set-up the network with a shared work area for pupils and one for staff. Staff and pupils are shown how to save work and access work from these areas
- Requires all users to always log off when they have finished working or are leaving the computer unattended and where a user finds a logged-on machine, we require them to always log-off and then log-on again as themselves
- Students are given a warning after 5 minutes of inactivity, after 10 minutes they are locked and 15 minutes of activity leads to logout. For staff this is 10 minutes for warning, 15 for lock and 8 hours for logout.
- We request that staff switch the computers off at the end of the day and we also automatically switch off all computers at 22.00 to save energy
- Has set-up the network so that users cannot download executable files / programmes
- Has blocked access to music andmedia download except those approved for educational purposes
- Scans all mobile equipment with anti-virus / spyware before it is connected to the network
- Makes clear that staff are responsible for ensuring that all equipment that goes home has the anti-virus and spyware software maintained up-to-date and the school provides them with a solution to do so
- Makes clear that staff are responsible for ensuring that any computer or laptop loaned to them by the school, is used solely to support their professional responsibilities and that they notify the school of any "significant personal use" as defined by HM Revenue & Customs
- Maintains equipment to ensure Health and Safety is followed e.g. projector filters cleaned by site manager / TA, equipment installed and checked by approvedsuppliers / LA electrical engineers
- Has integrated curriculum and administration networks, but access to the Management Information System is set-up so as to ensure staff users can only access modules related to their role

- Ensures that access to the school's network resources from remote locations by staff is restricted and access is only through school / LA approved systems
- Does not allow any outside agencies to access our network remotely except where there is a clear professional need and then access is restricted and is only through approved systems
- Provides pupils and staff with access to content and resources through the approved Learning Platform which staff and pupils access using their username and password
- Makes clear responsibilities for the daily back up of MIS and finance systems and other important files
- Has a clear disaster recovery system in place for critical data that includes a secure, remote back up of critical data that complies with external audit requirements
- Uses our broadband network for our CCTV system and have had the set-up completed by approved partners
- Uses the DfE secure s2s website for all CTF files sent to other schools
- Ensures that all pupil level data or personal data sent over the internet is encrypted or only sent within the approved secure system in our LA or through USO secure file exchange
- Follows ISP advice on Local Area and Wide Area security matters and firewalls and routers have been configured to prevent unauthorised use of our network
- Our wireless network has been secured to industry standard enterprise security level /appropriate standards suitable for educational use
- All computer equipment is installed professionally and meets health and safety standards
- Projectors are maintained so that the quality of presentation remains high
- Reviews the school ICT systems regularly with regard to health and safety and security

Passwords policy

- This school makes it clear that staff and pupils must always keep their password private and must not share it with others or leave it where others can find it
- All staff have their own unique username and private passwords to access school systems. Staff are responsible for keeping their password private
- We require staff and students to change their passwords on a yearly basis

E-mail

This school

- Provides staff with an email account for their professional use and makes it clear that personal email should be through a separate account
- Personal e-mail addresses of pupils or staff are not published on the school website. We encourage the use of anonymous or group e-mail addresses, for example info@schoolname.la.sch.uk / head@schoolname.la.sch.uk
- Will contact the police if one of our staff or pupils receives an e-mail that we consider is particularly disturbing or breaks the law.
- Will ensure that email accounts are maintained and up to date
- Reports messages relating to or in support of illegal activities to the relevant authority and if necessary to the police
- Knows that spam, phishing and virus attachments can make e-mails dangerous. We use a number of approved technologies to help protect users and systems in the school, including desktop anti-virus

product Sophos, plus direct email filtering for viruses, Trojans, pornography, phishing and inappropriate language

Pupils:

- We use the school email system with pupils and lock this down where appropriate using our own filtering rules
- Pupils are introduced to, and use e-mail as part of the ICT/Computing scheme of work
- Pupils are taught about the safety and 'netiquette' of using e-mail both in school and at home i.e. they are taught:
    - to 'Stop and Think Before They Click' and not open attachments unless sure the source is safe
    - that they should think carefully before sending any attachments
    - that they must immediately tell a teacher / responsible adult if they receive an e-mail which makes them feel uncomfortable, is offensive or bullying in nature
    - not to respond to malicious or threatening messages
    - not to delete malicious of threatening e-mails, but to keep them as evidence of bullying
    - not to arrange to meet anyone they meet through e-mail without having discussed with an adult and taking a responsible adult with them
- Pupils sign the school Agreement Form to say they have read and understood the e-safety rules, including e-mail and we explain how any inappropriate use will be dealt with

Staff:

- Staff can use personal email as well as their school email on the system.
- Staff should only use school e-mail systems for professional purposes
- We use secure email systems to send MIS data
- Staff know that e-mail sent to an external organisation must be written carefully, (and may require authorisation), in the same way as a letter written on school headed paper. That it should follow the school 'house-style':
    - the sending of multiple or large attachments should be limited, and may also be restricted by the provider of the service being used
    - the sending of chain letters is not permitted
    - embedding adverts is not allowed
- All staff sign our school Agreement Form AUP to say they have read and understood the e-safety rules, including e-mail and we explain how any inappropriate use will be dealt with

School website

- The Headteacher takes overall responsibility to ensure that the website content is accurate and the quality of presentation is maintained
- Uploading of information is restricted to our website authorisers and IT Support team
- The school web site complies with the statutory DfE guidelines for publications
- Most material is the school's own work; where other's work is published or linked to, we credit the sources used and state clearly the author's identity or status
- The point of contact on the web site is the school address, telephone number and we use a general email contact address. Home information or individual e-mail identities will not be published
- Photographs published on the web do not have full names attached

- We do not use pupils' names when saving images in the file names or in the tags when publishing to the school website
- We do not use embedded geodata in respect of stored images
- We expect teachers using school approved blogs or wikis to password protect them and run from the school website

Learning platform

- Uploading of information on the school's Learning Platform is shared between different staff members according to their responsibilities e.g. all class teachers upload information in their class areas
- Photographs and videos uploaded to the schools Learning Platform will only be accessible by members of the school community

Social networking

- Teachers are instructed not to run social network spaces for student use on a personal basis or to open up their own spaces to their students, but to use the school's preferred system for such communications

School staff will ensure that in private use:

- No reference should be made in social media to students, parents / carers or school staff
- They do not engage in online discussion on personal matters relating to members of the school community
- Personal opinions should not be attributed to the school or local authority
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

CCTV

- We have CCTV in the school as part of our site surveillance for staff and student safety. We will not reveal any recordings without permission except where disclosed to the police as part of a criminal investigation
- We use specialist lesson recording equipment on occasions as a tool to share best teaching practice. We do not reveal any such recordings outside of the staff and will not use for any other purposes

5. Data security: Management Information System access and Data transfer

Strategic and operational practices

At this school:

- The Head Teacher is the Senior Information Risk Officer (SIRO).
- Where data protection may have been compromised staff should report the incident to their line manager.
- All staff are DBS checked and records are held in one central record
- We ensure ALL the following school stakeholders sign an Acceptable Use Agreement form. Signed forms are kept in personnel files.
  - staff,
  - governors,
  - pupils
  - parents

This makes clear staffs' responsibilities with regard to data security, passwords and access.

- We follow LA guidelines for the transfer of any data, such as MIS data or reports of children, to professionals working in the Local Authority or their partners in Children's Services / Family Services, Health, Welfare and Social Services.
- School staff with access to setting-up usernames and passwords for email, network access and Learning Platform access are working within the approved system and follow the security processes required by those systems.
- We ask staff to undertake at least annual house-keeping to review, remove and destroy any digital materials and documents which need no longer be stored.

Technical Solutions

- There are secure area(s) on the network to store sensitive documents or photographs.
- We use the A2C site to securely transfer CTF pupil data files to other schools.
- We store any Protect and Restricted written material in a secure area
- All servers are in lockable locations
- We store any back-up tapes in a secure cupboard in a separate building
- We comply with the WEEE directive on equipment disposal by using an approved or recommended disposal company for disposal of equipment where any protected or restricted data has been held and get a certificate of secure deletion for any server that once contained personal data.
- Portable equipment loaned by the school (for use by staff at home), where used for any protected data, is disposed of through the same procedure.
- Paper based sensitive information is collected by secure data disposal service.

6. Equipment and Digital Content

Personal mobile phones and mobile devices

- The recording, taking and sharing of images, video and audio on any mobile phone is to be avoided; except where it has been explicitly agreed otherwise by the headteacher. Such authorised use is to be monitored and recorded. All mobile phone use is to be open to scrutiny and the headteacher is to be able to withdraw or restrict authorisation for use at any time if it is to be deemed necessary.
- All mobile phones and personally-owned mobile devices brought in to school are the responsibility of the device owner. The school accepts no responsibility for the loss, theft or damage of personally-owned mobile phones or mobile devices.
- Mobile phones and personally-owned devices are not permitted to be used in certain areas within the school site, e.g. changing rooms and toilets.
- Students' mobile phones will not be used during lessons or formal school time unless as part of an approved and directed curriculum-based activity with consent from a member of staff.
- No images or videos should be taken on mobile phones or personally-owned mobile devices without the prior consent of the person or people concerned. Any permitted images or files taken in school must be downloaded from the device and deleted in school before the end of the day

Students' use of personal devices

- The School strongly advises that student mobile phones should not be brought into school but accepts that there may be particular circumstances in which a parent wishes their child to have a mobile phone for their own safety.

- Student mobile phones which are brought into school must be turned off (not placed on silent) and stored out of sight on arrival at school. They must remain turned off and out of sight until the end of the day.

- If a student breaches the school policy then the phone or device will be confiscated and will be held in a secure place in the school office. Mobile phones and devices will be released in accordance with the school policy.
- Phones and devices must not be taken into examinations. Students found in possession of a mobile phone during an exam will be reported to the appropriate examining body. This may result in the student's withdrawal from either that examination or all examinations.
- If a student needs to contact his or her parents or carers, they will be allowed to use a school phone. Parents are advised not to contact their child via their mobile phone during the school day, but to contact the school office.
- Students should protect their phone numbers by only giving them to trusted friends and family members. Students will be instructed in safe and appropriate use of mobile phones and personally-owned devices and will be made aware of boundaries and consequences.
- Staff are not permitted to use their own mobile phones or devices for contacting children, young people or their families within or outside of the setting in a professional capacity.
- If members of staff have an educational reason to allow children to use mobile phones or a personally-owned device as part of an educational activity then it will only take place when approved by the line manager.
- If a member of staff breaches the school policy then disciplinary action may be taken.
- Where staff members are required to use a mobile phone for school duties, for instance in case of emergency during off-site activities, or for contacting students or parents, then a school mobile phone will be provided and used. In an emergency where a staff member doesn't have access to a school-owned device, they should use their own device and hide (by inputting 141) their own mobile number for confidentiality purposes.

Digital images and video
In this school:

- We gain parental / carer permission for use of digital photographs or video involving their child as part of the school agreement form when their daughter son joins the school
- We do not identify pupils in online photographic materials or include the full names of pupils in the credits of any published school produced video materials / DVDs
- Staff sign the school's Acceptable Use Policy and this includes a clause on the use of mobile phones / personal equipment for taking pictures of pupils
- If specific pupil photos (not group photos) are used on the school web site, in the prospectus or in other high profile publications the school will obtain individual parental or pupil permission for its long term use
- The school blocks/filters access to social networking sites or newsgroups unless there is a specific approved educational purpose
- Pupils are advised to be very careful about placing any personal photos on any 'social' online network space. They are taught to understand the need to maintain privacy settings so as not to make public, personal information.
- Pupils are taught that they should not post images or videos of others without their permission. We teach them about the risks associated with providing information with images (including the name of the file), that reveals the identity of others and their location, such as house number, street name or school. We teach them about the need to keep their data secure and what to do if they are subject to bullying or abuse.

Electronic Entry Systems

- We have electronic gates on all of the entrances to the site. These are controlled by RFID swipe cards. All staff are issued with swipe cards upon their employment, and are disabled at the end of their tenure.
- Sixth form students are also given swipe cards, but with more restricted hours of use, i.e. school hours and are disabled during summer (at the request of the head of sixth form).

ID Badges

- All staff are required to wear photographic ID badges.

Fingerprints

- Access to the cashless canteen system is via a fingerprint taken on joining the school
- All students' finger prints are entered on to the system unless permission is denied by the parent/guardian. The finger prints are not held in a graphic format, rather keypoints are taken from the finger, and converted into a number which will be unique to the user. This means that no graphic representation of the fingerprint is kept, and are thus only usable on our systems and useless outside of this.

Asset disposal

Ask Rick

- Details of all school-owned hardware will be recorded in a hardware inventory.
- Details of all school-owned software will be recorded in a software inventory.
- All redundant equipment will be disposed of through an authorised agency. This will include a written receipt for the item including an acceptance of responsibility for the destruction of any personal data.
- All redundant equipment that may have held personal data will have the storage media wiped.
- Disposal of any equipment will conform to The Waste Electrical and Electronic Equipment Regulations 2006 and/or The Waste Electrical and Electronic Equipment (Amendment) Regulations 2007. Further information can be found on the Environment Agency website.

Review and Monitoring

The e-safety policy is referenced within other school policies including the following: ICT and Computing policy, Child Protection policy, Anti-Bullying policy, Behaviour policy, and the PSHCE policy.

- The school has two safeguarding coordinators who are introduced to new staff when they start and whose names , photos and extension numbers are up in every classroom.
- The e-safety policy will be reviewed annually or when any significant changes occur with regard to the technologies in use within the school

APPENDIX 1: E-SAFETY AGREEMENT FORM: PARENTS

Parent / carer name: _____

Student name(s): _____

As the parent or legal guardian of the above student(s), I grant permission for my daughter to have access to use the Internet, the school e-mail and other ICT facilities at school.

I know that my daughter has signed an e-safety agreement form and that they have a copy of the 14 'rules for responsible ICT use'.

I accept that ultimately the school cannot be held responsible for the nature and content of materials accessed through the Internet and mobile technologies, but I understand that the school will take every reasonable precaution to keep pupils safe and to prevent students from accessing inappropriate materials. These steps include using an educationally filtered service, employing appropriate teaching practice and teaching e-safety skills to students.

I understand that the school can check my daughter's computer files, and the Internet sites they visit, and that if they have concerns about their e-safety or e-behaviour that they will contact me.

I will support the school by promoting safe use of the Internet and digital technology at home and will inform the school if I have any concerns over my child's e-safety.

Parent / guardian signature: _____

Date: _____

Use of digital images - photography and video

To comply with the Data Protection Act 1998, we need your permission before we can photograph or make recordings of your daughter

I also agree to the school using photographs of my child or including them in video material, as described in the document 'Use of digital and video images'. I have read and understood this document. I understand that images will only be used to support learning activities or in publicity that reasonably promotes the work of the school, and for no other purpose.

Parent / Carer signature: _____ Date: ___/___/___

We follow the following rules for any external use of digital images:

If the pupil is named, we avoid using their photograph.
If their photograph is used, we avoid naming the pupil.

Where showcasing examples of pupils work we only use their first names, rather than their full names.

If showcasing digital video work to an external audience, we take care to ensure that pupils aren't referred to by name on the video, and that pupils' full names aren't given in credits at the end of the film.
Only images of pupils in suitable dress are used.
Staffs are not allowed to take photographs or videos on their personal equipment.

Examples of how digital photography and video may be used include:

Your child being photographed (by the classroom teacher, teaching assistant or another child) as part of a learning activity;
e.g. photographing children at work and then sharing the pictures on the Interactive whiteboard in the classroom allowing the children to see their work and make improvements.
Your child's image for presentation purposes around the school;
e.g. in school wall displays and PowerPoint© presentations to capture images around the school or in the local area as part of a project or lesson.
Your child's image being used in a presentation about the school and its work in order to share its good practice and celebrate its achievements, which is shown to other parents, schools or educators;
e.g. within a CDROM / DVD or a document sharing good practice; in our school prospectus or on our school website. In rare events, your child's could appear in the media if a newspaper photographer or television film crew attend an event.
Note: If we, or you, actually wanted your child's image linked to their name we would contact you separately for permission, e.g. if your child won a national competition and wanted to be named in local or government literature.

Appendix 2: Pupil Acceptable Use Agreement

These rules will keep everyone safe and help us to be fair to others;

- I will only use the school's computers for schoolwork, homework and as directed;
- I will not bring files into school (on removable media or online) without permission or upload inappropriate material to my workspace;
- I will only edit or delete my own files and not view, or change, other people's files without their permission;
- I will keep my logins, IDs and passwords secret and will change them when requested;
- I will use the Internet responsibly and will not visit web sites I know to be banned by the school. I am also aware that during lessons I should visit web sites that are appropriate for my studies;
- I will only e-mail people I know, or those approved by my teachers;
- The messages I send, or information I upload, will always be polite and sensible;
- I will not open attachments, or download a file, unless I have permission or I know and trust the person that has sent them;
- I will not give my home address, phone number, send photographs or video, or give any other personal information that could be used to identify me, my family or my friends, unless a trusted adult has given permission;
- I will never arrange to meet someone I have only ever previously met on the Internet or by email or in a chat room, unless I take a trusted adult with me;
- If I see anything I am unhappy with or I receive a message I do not like, I will not respond to it but I will save it and talk to a teacher / trusted adult;
- I am aware that some websites and social networks have age restrictions and I should respect this;
- I am aware that my online activity at all times should not upset or hurt other people and that I should not put myself at risk;
- I will respect that others need to use the computers. I will log off when I have finished using them and not interfere with their proper operation;
- I agree that the use of computers is monitored for the protection of both others and myself.

I have read and understand these rules and agree to them.

Signed:

Date:

Appendix 3: Acceptable Use Policy (AUP): Staff Agreement Form

Covers use of digital technologies in school: i.e. email, Internet, intranet and network resources, learning platform, software, equipment and systems.

- I will only use the school's digital technology resources and systems for Professional purposes or for uses deemed 'reasonable' by the Head and Governing Body.
- I will not reveal my password(s) to anyone other than ICT Support staff if necessary.
- I will change my password on a regular basis, as stated in the policy, and I will use a strong password
- If leaving the computer unattended I will lock the computer to prevent unauthorized access.
- I will not allow unauthorised individuals to access email / Internet / intranet / network, or other school / LA systems.
- I will ensure all documents, data etc., are saved, accessed and deleted in accordance with the school's network and data protection policy.
- I will not engage in any online activity that may compromise my professional responsibilities.
- I will only use the approved, secure email system(s) for any school business.
  (Which is currently: outlook)
- I will only use the approved school email, school MLE or other school approved communication systems with pupils or parents/carers, and only communicate with them on appropriate school business.

- I will not browse, download or send material that could be considered offensive to colleagues.
- I will report any accidental access to, or receipt of inappropriate materials, or filtering breach to Esafety officer (Angela Stone).
- I will not download any software or resources from the Internet that can compromise the network, or are not adequately licensed.
- I will not connect a computer, laptop or other device (including USB flash drive), to the network / Internet that does not have up-to-date anti-virus software, and I will keep any 'loaned' equipment up-to-date, using the school's recommended anti-virus, firewall and other ICT 'defence' systems.
- I will not use personal digital cameras or camera phones for taking and transferring images of pupils or staff without permission and will not store images at home without permission.
- I will use the school's Learning Platform in accordance with school advice.
- I will ensure that any private social networking sites / blogs etc that I create or actively contribute to are not confused with my professional role.
- I agree and accept that any computer or laptop loaned to me by the school, is provided solely to support my professional responsibilities and that I will notify the school of any "significant personal use" as defined by HM Revenue & Customs.
- I will ensure any confidential data that I wish to transport from one location to another is protected by encryption and that I follow school data security protocols when using any such data at any location.
- I understand that data protection policy requires that any information seen by me with regard to staff or pupil information, held within the school's information management system, will be kept private and confidential, EXCEPT when it is deemed necessary that I am required by law to disclose such information to an appropriate authority.
- I will embed the school's e-safety curriculum into my teaching.
- I will only use LA systems in accordance with any corporate policies.
- I understand that all Internet usage / and network usage can be logged and this information could be made available to my manager on request.
- I understand that failure to comply with this agreement could lead to disciplinary action.

User Signature
I understand that it is my responsibility to ensure that I remain up-to-date and read and understand the school's most recent e-safety policies.

I agree to abide by all the points above.

I wish to have an email account; be connected to the Intranet & Internet; be able to use the school's ICT resources and systems.

Signature …… Date……..

Full Name…….. (printed)

Job title ……..

Authorised Signature:
I approve this user to be set-up.

Signature …… Date……..

Full Name …….. (printed)

APPENDIX 4: ACCEPTABLE USE POLICY (AUP): AGREEMENT FORM FOR ADULTS WORKING WITH CHILDREN – IN PAID OR VOLUNTARY CAPACITY

Covers use of digital technologies in Brentford School for Girls: i.e. email, Internet, intranet and network resources, learning platform, software, equipment and systems.

- I will only use the Brentford School for Girls digital technology resources and systems for Professional purposes or for uses deemed 'reasonable' by Brentford School for Girls;
- I will not reveal my password(s) to anyone other than ICT support and will change the password as stated in the policy. I will use a strong password;
- If leaving the computer unattended I will lock the computer to prevent unauthorized access;
- I will not allow unauthorised individuals to access email / Internet / intranet / network, or other Brentford School for Girls systems;
- I will ensure all documents, data etc., are saved, accessed and deleted in accordance with the Brentford School for Girls data security and confidentiality protocols;
- I will not engage in any online activity that may compromise my professional responsibilities;
- I will only use the approved, secure email system(s) for any Brentford School for Girls business;
- I will only use the approved Brentford School for Girls email or other Brentford School for Girls approved communication systems with young people or parents/carers, and only communicates with them on appropriate Brentford School for Girls business;
- I will not browse, download or send material that could be considered offensive to colleagues;
- I will report any accidental access to, or receipt of inappropriate materials, or filtering breach to the appropriate contact;
- I will not download any software or resources from the Internet that can compromise my computer, or are not adequately licensed;
- I will not use personal digital cameras or camera phones for taking and transferring images of young people without permission and will not store images at home without permission;
- I will ensure that any private social networking sites / blogs etc that I create or actively contribute to are not confused with my professional role;
- I agree and accept that any computer or laptop loaned to me by the Brentford School for Girls, is provided solely to support my professional responsibilities and that I will notify the school of any "significant personal use" as defined by HM Revenue & Customs;
- I will ensure any confidential data that I wish to transport from one location to another is protected by encryption and that I follow Brentford School for Girls data security protocols when using any such data at any location;
- I understand that data protection policy requires that any information seen by me with regard to young peoples information, will be kept private and confidential, EXCEPT when it is deemed necessary that I am required by law to disclose such information to an appropriate authority;
- I will embed the e-safety messages for adults and young people into my area of work;
- I understand that all Internet usage may be logged and this information could be made available to my manager on request;
- I understand that failure to comply with this agreement could lead to disciplinary action.

User Signature

I understand that it is my responsibility to ensure that I remain up-to-date and read and understand the most recent e-safety policies.

I

agree to abide by all the points above.

Signature …….. Date……..

Full Name …….. (printed)

Job title …….

APPENDIX 5 PROTOCOLS : WHAT DO WE DO IF?

An inappropriate website is accessed unintentionally in school by a teacher or child.

1. Play the situation down; don't make it into a drama.
2. Report to the e- safety coordinator and decide whether to inform parents of any children who viewed the site.
3. Inform ICT Support and ensure the site is filtered
4. Inform the LA if the filtering service is provided via an LA.

An inappropriate website is accessed intentionally by a child.

1. Refer to the acceptable use policy that was signed by the child, and apply agreed sanctions.
2. Notify the parents of the child.
3. Inform the school technicians and ensure the site is filtered if need be.
4. Inform the LA if the filtering service is provided via an LA

An adult uses School IT equipment inappropriately.

1. Ensure you have a colleague with you, do not view the misuse alone.
2. Report the misuse immediately to the Head Teacher / e-safety coordinator in Head teachers' absence and ensure that there is no further access to the PC or laptop.
3. If the material is offensive but not illegal, the head teacher should then:
    - Remove the PC to a secure place.
    - Instigate an audit of all ICT equipment by the school's ICT managed service providers to ensure there is no risk of pupils accessing inappropriate materials in the school.
    - Identify the precise details of the material.
    - Take appropriate disciplinary action (contact Personnel/Human Resources).
    - Inform governors of the incident.

In an extreme case where the material is of an illegal nature:

- Contact the local police or High Tech Crime Unit and follow their advice.
- If requested to remove the PC to a secure place and document what you have done.

A bullying incident directed at a child occurs through email or mobile phone technology, either inside or outside of school time.

1. Advise the child not to respond to the message.
2. Refer to relevant policies including e-safety and anti-bullying policy.
3. Secure and preserve any evidence.
4. Take the matter to the e-safety coordinator who may need to:
    - Inform the sender's e-mail service provider.
    - Notify parents of the children involved.
    - Consider delivering a parent workshop for the school community.
    - Inform the police if necessary.
    - Inform the LA e-safety officer / head teacher.

Malicious or threatening comments are posted on an Internet site about a pupil or member of staff.

1. The e-safety officer should be informed immediately. They will:
    - Request the comments be removed if the site is administered externally.
    - Secure and preserve any evidence.
    - Send all the evidence to CEOP at ww.ceop.gov.uk/contact_us.html.
    - Endeavour to trace the origin and inform police as appropriate.
    - Inform LA e-safety officer / head teacher.

You are concerned that a child's safety is at risk because you suspect someone is using communication technologies (such as social networking sites) to make inappropriate contact with the child

1. Report to and discuss with the named child protection officer/ e-safety officer in school and agree who will
    - Contact parents.
    - Advise the child on how to terminate the communication and save all evidence.
    - Contact CEOP http://www.ceop.gov.uk/
    - Consider the involvement of police and social services.
    - Inform LA e-safety officer/ head teacher.
2. Consider delivering a parent workshop for the school community.

Children should be confident in a no-blame culture when it comes to reporting inappropriate incidents involving the internet or mobile technology: they must be able to do this without fear.

Appendix 6

Possible infringements and suggested potential sanctions for students and staff.

STUDENTS

Category A infringements
Use of non-educational sites during lessons
Unauthorised use of email
Unauthorised use of mobile phone (or other new technologies) in lessons e.g. to send texts to friends
Use of unauthorised instant messaging / social networking sites
Disclosure of password to another student
Use of another student's password

Possible Sanctions
The class teacher will deal with the infringement within the classroom according to the behaviour policy. Any use of mobile phone will result in the phone being confiscated and returned at the end of the day (first offence).

Category B infringements
Continued use of non-educational sites during lessons after being warned
Continued unauthorised use of email after being warned
Continued unauthorised use of mobile phone (or other new technologies) after being warned
Continued use of unauthorised instant messaging / chatrooms, social networking sites, NewsGroups
Use of Filesharing software e.g. Vanbasco, BitTorrent, LimeWire, etc
Accidentally corrupting or destroying others' data without notifying a member of staff of it
Accidentally accessing offensive material and not logging off or notifying a member of staff of it
Disabling of ICT equipment, or damaging ICT equipment accidentally due to carelessness or installing or attempting to install software
Use of a member of staff's password

Possible Sanctions:
Referred to Subject Leader initially. This may lead to subject detention / removal of Internet access rights for a period / removal of phone until end of day / contact with parent. If necessary, refer to safeguarding coordinator.

Category C infringements
Deliberately corrupting or destroying someone's data, violating privacy of others
Sending an email or MSN message that is regarded as harassment or of a bullying nature (one-off)
Deliberately trying to access offensive or pornographic material
Any purchasing or ordering of items over the Internet
Transmission of commercial or advertising material
Damaging ICT equipment wilfully
Interfering, or attempting to interfere with network security

Possible Sanctions
Referred to the safeguarding coordinator immediately.
This may lead to removal of Internet and / or Learning Platform access rights for a period of time / contact with parents / internal exclusion / external exclusion.
If inappropriate web material is accessed, the safeguarding coordinator should also inform the Network Manager to:
Ensure appropriate technical support filters the site
Inform LA / Synetrix as appropriate

Category D infringements

Continued sending of emails or MSN messages regarded as harassment or of a bullying nature after being warned
Deliberately accessing, downloading and disseminating any material deemed offensive, obscene, defamatory, racist, homophobic or violent
Receipt or transmission of material that infringes the copyright of another person or infringes the conditions of the Data Protection Act, revised 1988
Bringing the school name into disrepute

Possible Sanctions
Referred to safeguarding coordinator / Head Teacher immediately.
This may lead to contact with parents / possible exclusion / removal of equipment / refer to Community Police Officer.
The safeguarding coordinator should also:

- Secure and preserve any evidence
- Inform the sender's e-mail service provider

STAFF

Category A infringements (Misconduct)
Excessive use of internet for personal activities not related to professional development e.g. online shopping, personal email, instant messaging etc.
Use of personal data storage media (e.g. USB memory sticks) without considering access and appropriateness of any files stored.
Not implementing appropriate safeguarding procedures.
Any behaviour on the internet that compromises the staff member's professional standing in the school and community.
Misuse of first level data security, e.g. wrongful use of passwords.
Breaching copyright or license e.g. installing unlicensed software on network.

Possible Sanctions
Referred to line manager / Head teacher
Warning given

Category B infringements (Gross Misconduct)
Serious misuse of, or deliberate damage to any school / council computer hardware or software
Any deliberate attempt to breach data protection or computer security rules
Deliberately accessing, downloading and disseminating any material deemed offensive, obscene, defamatory, racist, homophobic or violent
Receipt or transmission of material that infringes the copyright of another person or infringes the conditions of the Data Protection Act, revised 1988
Bringing the school name into disrepute

Possible Sanctions
Referred to Head teacher / Governors and follow school disciplinary procedures; report to LA Personnel/ Human resources, report to police.

Other safeguarding actions:
Remove the PC to a secure place to ensure that there is no further access to the PC or laptop
Instigate an audit of all ICT equipment by an outside agency, such as the schools ICT managed service providers, to ensure there is no risk of pupils accessing inappropriate materials in the school.
Identify the precise details of the material

If a member of staff commits an exceptionally serious act of gross misconduct they should be instantly suspended. Normally there will be an investigation before disciplinary action is taken for any alleged offence. As part of that the member of staff will be asked to explain their actions and these will be considered before any disciplinary action is taken

Schools are likely to involve external support agencies as part of these investigations e.g. an ICT technical support service to investigate equipment and data evidence, the Local Authority Human Resources team

CHILD PORNOGRAPHY FOUND?

In the case of Child Pornography being found, the member of staff should be immediately suspended and the police should be called: see the free phone number 0808 100 00 40 at:
http://www.met.police.uk/childpornography/index.htm
Anyone may report any inappropriate or potentially illegal activity or abuse with or towards a child online to the Child Exploitation and Online Protection (CEOP):
http://www.ceop.gov.uk/reporting_abuse.html
http://www.iwf.org.uk

HOW WILL STAFF AND STUDENTS BE INFORMED OF THESE PROCEDURES?

Procedures will be fully explained and included within the school's e-safety policy. All staff will be required to sign the school's e-safety policy acceptance form;
Students will be taught about responsible and acceptable use and given strategies to deal with incidents so they can develop 'safe behaviours'
The school's e-safety policy will be made available and explained to parents, and parents will sign an acceptance form when their child starts at the school
Information on reporting abuse / bullying etc. will be made available by the school for pupils, staff and parents when requested
Staff are issued with the 'What to do if?' guide on e-safety issues.

APPENDIX 7: USING NEW TECHNOLOGY - HINTS AND TIPS FOR ADULTS WORKING WITH YOUNG PEOPLE

Social Networking hints and tips

- Manage your social networking sites so that only invited friends can, only see your details, photographs etc.
- Have a neutral picture of yourself as your profile image. Don't post embarrassing material.
- Reject or ignore friendship requests from students or young people (or their parents) that you work with. Remember ex-pupils may still have friends at your school.
- Exercise caution – for example in Facebook if you write on a friends 'wall' all their friends can see your comment – even if they are not your friend.
- There is a separate privacy setting for Facebook groups & networks, you might have your profile set to private, but not for groups & networks. If you join a group or network everyone in the group or network will be able to see your profile.
- If you have younger family members on your social networking group who are friends with your students or pupils be aware that posts that you write will be visible to them.
- If you wish to set up a social networking site for a school project create a new user profile for this, do not use your own profile.
- If you or a friend are 'tagged' in an online photo album (Facebook, Flickr or similar) the whole photo album will be visible to their friends, your friends and anyone else tagged in the same album.
- You do not have to be friends with someone to be tagged in their photo album. - If you are tagged in a photo you can remove the tag, but not the photo.
- Photo sharing web sites may not have privacy set as default.
- Your friends may take and post photos you are not happy about. You need to speak to them first, rather than contacting a web site. If you are over 18 the web site will only look into issues that contravene their terms and conditions.
- Once something is on the Internet, even if you remove it, the chances are it has already been snapshotted by a 'web crawler' and it will always be there.

Wider Internet hints and tips

- Never tell anyone your passwords.
- Be careful how you choose passwords, most are very predictable. It is easy to find personal details online that might give password clues. It is recommended that you include capital letters, punctuation, lower

case letters and numbers – avoid birthdates, names, pets, addresses etc. It is best to avoid any word found in a dictionary.

- Keep all professional work and transactions completely separate from private. Create a web-based email account for private online business, such as online shopping and ensure you use your school / work email only for any professional communications.
- Be careful when form filling online… do you know whom the data is for? Only answer 'required 'questions, do not just give out information because you have been asked for it.
- Check the padlock symbol on the browser before putting in any sensitive information such as credit card details. Unless the padlock is in the closed position, the details will be sent in "clear text" and could be intercepted by a third party.
- Never verify banking details online.
- When you need to use a 'name' online consider what name you use. In a professional context you would probably use your full name, but in other contexts you may decide to use an alias to protect your identity. If so make sure it is appropriate.
- If you think someone is impersonating you on Facebook or similar, report it. Impersonation usually breaches the terms and conditions – you will need to know the specific URL or user name.
- Use legal sites for downloading music, films etc., such as iTunes.
- File sharing sites are not illegal but sharing of copyright material is. Downloading of illegal music and film downloading also leaves you at a huge risk of viruses. Even if you subscribe to a file sharing web site it does not mean that your downloading becomes legal.
- When you log-into a web site, unless your computer is exclusive to you, don't tick boxes that say 'remember me'.
- Don't leave yourself logged into your computer, software or websites. If you have to move away from your computer, log out or lock your pc.
- Don't give your username and password to anyone such as to a supply teacher / temporary member of staff – make sure your school has a guest login for visiting staff.
- Your school or work laptop (or other equipment) should not be used by friends and family.

Using internet in the classroom:

- Try to provide pupils with direct links embedded into 'pages' in a document
- If you do need to undertake Internet searches (including Internet image searches), rehearse before you use in class. Think about search terms. Even the most innocuous term can bring up adult material.
- Use child-friendly search engines with younger pupils. Older students will use a variety of search engines at home, you are a role model for them in good use of a search engine. Look for opportunities to teach young people how to use search engines responsibly.
- When checking out web content make sure you are not displaying it on the interactive whiteboard or via a projector – research away from pupils.
- Watch YouTube (or any) videos before you use them in the classroom.
- If you use YouTube (or any) videos, find out how to embed it using the 'Source' rather than a page link, as that exposes pupils to other content.
- If you cut and paste or save content from the Internet or other peoples files make sure you remove the hyperlinks embedded in the text, or attached to images.
- If you want to use a clip download it (if legal & copyright allows), it might not be there next time you look for it.
- If you use your own equipment in school (such as cameras or laptops), ensure senior leadership have given you permission and make sure that school files (photographs etc) are downloaded and stored in school, not at home.
- Do not take stored pupil photos or information home. If for any reason you need to ensure you have senior leadership's permission, and ensure it is on an encrypted device..
- You need to be a role model for copyright. Make sure you use multimedia resources appropriately, don't just 'grab stuff' off the Internet.

Email hints and tips

- If you get an email from someone or a company that you have never heard of and it asks you to reply to unsubscribe, don't. By unsubscribing you will verify that you exist. Just ignore the email. If they carry on emailing use email rules to block the sender.

- Only open Email attachments from trusted sources, you won't get a virus from the initial email text, but it may be contained in an attachment.
- If emails from friends or acquaintances start to become unsuitable – say something before you receive something really problematic.
- Don't give out private email addresses to students.

Phone hints and tips

- Don't give out your mobile number or home number to students.
- If you have a Bluetooth phone do you know if Bluetooth is turned on or off? If it is on is there a password? Open un-passworded Bluetooth means anyone else with Bluetooth in range can read the content of your phone or device.
- Many hand held games consoles have wireless and Bluetooth and can be used to make contact from 'stranger' devices within range.

Appendix 7: Search and Confiscation guidance from DfE

https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/279245/searching_screening_confiscation_advice_feb14.pdf

Statutory guidance for dealing with electronic devices

- Where the person conducting the search finds an electronic device they may examine any data or files on the device if they think there is a good reason to do so. Following an examination, if the person has decided to return the device to the owner, or to retain or dispose of it, they may erase any data or files, if they think there is a good reason to do so.
- The member of staff must have regard to the following guidance issued by the Secretary of State when determining what is a "good reason" for examining or erasing the contents of an electronic device:
- In determining a 'good reason' to examine or erase the data or files the staff member must reasonably suspect that the data or file on the device in question has been, or could be, used to cause harm, to disrupt teaching or break the school rules.
- If inappropriate material is found on the device it is up to the teacher to decide whether they should delete that material, retain it as evidence (of a criminal offence or a breach of school discipline) or whether the material is of such seriousness that it requires the involvement of the police.