`

Barnwell School

Policy for ICT Acceptable Use Incorporating eSafety, Data Security & Disposal of ICT Equipment

Reviewed – February 2020

To be reviewed – February 2022

Contents:

Introduction

ICT in the 21st Century is seen as an essential resource to support learning and teaching, as well as playing an important role in the everyday lives of children, young people and adults. Consequently, schools need to build in the use of these technologies in order to arm our young people with the skills to access life-long learning and employment.

Information and Communications Technology covers a wide range of resources including; web-based and mobile learning. It is also important to recognise the constant and fast paced evolution of ICT within our society as a whole. Currently the internet technologies children and young people are using both inside and outside of the classroom include:

- Websites
- Learning Platforms and Virtual Learning Environments
- E-mail and Instant Messaging
- Chat Rooms and Social Networking
- Blogs and Wikis
- Podcasting
- Video Broadcasting
- Music Downloading
- Gaming
- Mobile/ Smart phones with text, video and/ or web functionality
- Other mobile devices with web functionality

Whilst exciting and beneficial both in and out of the context of education, much ICT, particularly web-based resources, are not consistently policed. All users need to be aware of the range of risks associated with the use of these Internet technologies.

At Barnwell**,** we understand the responsibility to educate our students on eSafety issues; teaching them the appropriate behaviours and critical thinking skills to enable them to remain both safe and legal when using the internet and related technologies, in and beyond the context of the classroom.

Barnwell School holds personal data on learners, staff and other people to help them conduct their day-to-day activities. Some of this information is sensitive and could be used by another person or criminal organisation to cause harm or distress to an individual. The loss of sensitive information can result in media coverage, and potentially damage the reputation of Barnwell School. This can make it more difficult for Barnwell School to use technology to benefit learners.

Everybody at Barnwell school has a shared responsibility to secure any sensitive information used in their day to day professional duties and even staff not directly involved in data handling should be made aware of the risks and threats and how to minimise them.

Both this policy and the Acceptable Use Agreement (for all staff, governors, visitors and students) are inclusive of both fixed and mobile internet; technologies provided by Barnwell school (such as PCs, laptops, personal digital assistants (PDAs), tablets, webcams, whiteboards, voting systems, digital video equipment, etc); and technologies owned by students and staff, but brought onto school premises (such as laptops, mobile phones, mobile devices, PDAs and portable media players, etc).

Monitoring

Authorised ICT staff may inspect any ICT equipment owned or leased by the School at any time without prior notice. If you are in doubt as to whether the individual requesting such access is authorised to do so, please ask for their identification badge and contact their department. Any ICT authorised staff member will be happy to comply with this request. Authorised ICT Staff are named in Authorised Staff.

ICT authorised staff may monitor, intercept, access, inspect, record and disclose telephone calls, e-mails, instant messaging, internet/intranet use and any other electronic communications (data, voice or image) involving its employees or contractors, without consent, to the extent permitted by law. This may be to confirm or obtain School business related information; to confirm or investigate compliance with School policies, standards and procedures; to ensure the effective operation of School ICT; for quality control or training purposes; to comply with a Subject Access Request under the Data Protection Act 1998, or to prevent or detect crime.

ICT authorised staff may, without prior notice, access the e-mail or voice-mail account where applicable, of someone who is absent in order to deal with any business-related issues retained on that account.

All monitoring, surveillance or investigative activities are conducted by ICT authorised staff and comply with the Data Protection Act 1998, the Human Rights Act 1998, the Regulation of Investigatory Powers Act 2000 (RIPA) and the Lawful Business Practice Regulations 2000.

Please note that personal communications using School ICT may be unavoidably included in any business communications that are monitored, intercepted and/or recorded.

Breaches

A breach or suspected breach of policy by a School employee, contractor or student may result in the temporary or permanent withdrawal of School ICT hardware, software or services from the offending individual.

For staff any policy breach is grounds for disciplinary action in accordance with the school Disciplinary Procedure or, for Support Staff, in their Probationary Period as stated.

Policy breaches may also lead to criminal or civil proceedings.

The Information Commissioner's powers to issue monetary penalties came into force on 6 April 2010, allowing the Information Commissioner's office to serve notices requiring organisations to pay up to £500,000 for serious breaches of the Data Protection Act.

The data protection powers of the Information Commissioner's Office are to:

- Conduct assessments to check organisations are complying with the Act;
- Serve information notices requiring organisations to provide the Information Commissioner's Office with specified information within a certain time period;
- Serve enforcement notices and 'stop now' orders where there has been a breach of the Act, requiring organisations to take (or refrain from taking) specified steps in order to ensure they comply with the law;
- Prosecute those who commit criminal offences under the Act;
- Conduct audits to assess whether organisations' processing of personal data follows good practice,
- Report to Parliament on data protection issues of concern

For pupils, reference will be made to the school's behaviour policy.

Incident Reporting

Any security breaches or attempts, loss of equipment and any unauthorised use or suspected misuse of ICT must be immediately reported to the school's relevant responsible person. Additionally, all security breaches, lost/stolen equipment or data (including remote access and PINs), virus notifications, unsolicited emails, misuse or unauthorised use of ICT and all other policy non-compliance must be reported to the relevant responsible person. The relevant responsible individuals in the school are Tony Fitzpatrick Executive Headteacher, Matt Roberts Head of School, Maria Townsend Deputy Headteacher and Karen Palin Network Manager.

Acceptable Use Agreement: Students – Secondary

Student Acceptable Use Agreement / eSafety Rules

- I will only use ICT systems in school, including the internet, email, digital video, mobile technologies, etc, for school purposes.
- I will not download or install software on school technologies.
- I will only log onto the school network with my own user name and password.
- I will follow the schools ICT security system and not reveal my passwords to anyone and change them regularly.
- I will only use my school email address whilst in school for school purposes.
- I will make sure that all ICT communications with students, teachers or others is responsible and sensible.
- I will be responsible for my behaviour when using the school network/internet. This includes resources I access and the language I use.
- I will not deliberately browse, download, upload or forward material that could be considered offensive or illegal. If I accidentally come across any such material I will report it immediately to my teacher.
- I will ensure that any removable media I use at school will not contain any material that could be considered offensive or illegal and I understand the media can be subject to school security checks.
- I will not give out any personal information such as name, phone number, address, interests, schools or clubs or any personal image. I will not arrange to meet someone unless this is part of a school project approved by my teacher or if outside school, parent/carer.
- Images of students and/or staff will only be taken, stored and used for school purposes in line with school policy and not be distributed outside the school network.
- I will ensure that my online activity, both in school and outside school, will not cause my school, the staff, students or others distress or bring into disrepute.
- I will support the school approach to online safety and not deliberately upload or add images, video, sounds or text that could upset or offend any member of the school community.
- I will respect the privacy and ownership of others' work on-line at all times.
- I will not attempt to bypass the internet filtering system.
- I will only store files on the school network that are for my studies/subjects at school
- I will use the school network responsibility as instructed by my teachers
- I understand that everything I search for, access, post or receive online can be traced now and in the future. My activity can be monitored and logged and if necessary shared with teachers, parents/carers and then police if necessary. I know it is essential that I build a good online reputation.

- I understand that these rules are designed to keep me safe and that if they are not followed, school sanctions will be applied and my parent/carer may be contacted.

- I should never post photographs, videos or livestream without permission of all parties involved.
- I will not upload images, videos, sounds or words that could upset, now or in the future, any member of the school community, as this is cyberbullying.
- I will be respectful to everyone online and will not cause distress to anyone in the school community or bring the school into disrepute.
- I will report hurtful behaviour online and have the right to block and say no to any inappropriate or upsetting request.
- I will not lie about my agree in order to sign up for age inappropriate games, apps or social networks.
- I understand that not everything I see or hear online is true, accurate and genuine and that some people of the internet and not who they say they are. I will gain permission from parents/carers before arranging to meet someone I only know on the internet.
- I understand that these rules are designed to keep me safe and that if they are not followed, school sanctions will be applied and my parent/carer may be contacted. If I break the law the police may be informed.

Dear Parent/Carer

ICT including the internet, email and mobile technologies have become an important part of learning in our school. We expect all students to be safe and responsible when using any ICT. It is essential that students are aware of eSafety and know how to stay safe when using any ICT.

Students are expected to read and discuss this agreement with their parent or carer and then to sign and follow the terms of the agreement. Any concerns or explanation can be discussed with their class teacher or the school eSafety coordinator.

Please return the bottom section of this form to school for inclusion in your child's records.

Student and Parent/Carer Acceptable Use Agreement and eSafety Rules

We have discussed this document and ……(student name) agrees to follow the eSafety rules and to support the safe and responsible use of ICT at Barnwell School.

Parent/carer signature…….

Student signature……

Form…….. Date……..

Staff, Governor and Visitor Acceptable Use Agreement / Code of Conduct

ICT and the related technologies such as email, the internet and mobile devices are an expected part of our daily working life in school. The policy is designed to ensure that all staff are aware of their professional responsibilities when using any form of ICT. All staff are expected to sign this policy and adhere at all times to its contents. Any concerns or clarification should be discussed with school eSafety coordinator.

- I will only use the school's email / Internet / Intranet and any related technologies for professional purposes or for uses deemed 'reasonable' by the Head or Governing Body.
- I will comply with the ICT system security and not disclose any passwords provided to me by the school or other related authorities.
- I will ensure that all electronic communications with students and staff are compatible with my professional role.
- I will not give out my own personal details, such as mobile phone number and personal email address to students.
- I will only use the approved, secure email system for any school business.
- I will ensure that personal data (such as data held on SIMS) is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely. Personal data can only be taken out of school or accessed remotely when authorised by the Head or Governing Body.
- I will not install any hardware or software without permission of the Network Manager.
- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.
- Images of students and/or staff will only be taken, stored and used for professional purposes inline with school policy and with written consent of the parent, carer or staff member. Images will not be distributed outside the school network without the permission of the parent/carer, member of staff or Headteacher.
- I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available, on request, to my Line Manager or Headteacher.
- I will ensure that any removable media I use at school will not contain any material that could be considered offensive or illegal and I understand the media can be subject to school security checks.
- I will support the school approach to online safety and not deliberately upload or add any images, video, sounds or text that could upset or offend any member of the school community.
- I will respect copyright and intellectual property rights.
- I will ensure that my online activity, both in school and outside school, will not bring my professional role into disrepute.
- I will support and promote the school's eSafety policy and help students to be safe and responsible in their use of ICT and related technologies.
- I understand the need to separate my professional role from my private friendships; in my professional capacity I will not become 'friends' with parents/carers of pupils

on social networks. I will also ensure my private account will never undermine or disparage the school, its staff, governors, parents/carers or pupils. Privilege information must remain confidential. I will not upload any material about or reference the school or its community on my personal social network.

- I will follow the data protection outlined in GTPR policy. These include photographs, personal data and personal and sensitive data.
- I understand that as a member of staff I should at no time put myself in a position where safeguarding allegations can be made against me as a result of my personal device or personal accounts. I understand that the use oof personal devices in school is at the discretion of the headteacher.
- I understand that this forms part of the terms and conditions set out in my contract of employment.

User signature

I agree to follow this code of conduct and to support the safe use of ICT throughout the school.

Signature…….Date……..

Third Party IT Code of Conduct

There are times when third parties (e.g. lettings, visitors) request the use of a limit user network account to access the internet only or the use of the school's Guest WIFI.
When such an account has been granted the following policy is applied:

- The account's permitted use is for a limited period only.
- The school's internet and related technologies are for professional purposes only and agreed in advance with the Network Manager before the account is assigned.
- The account cannot be used for the conduct of any personal business.
- The account and password cannot be passed on.
- It is prohibited to install any hardware or software on any school device.
- It is prohibited to browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory and subject to the computer misuse act and data protection act.
- Be aware that the use of the internet and other related technologies are monitored and logged and will be made available to relevant personal within the school and to the guest's own organisation they are representing.

User signature
I agree to follow this code of conduct and to support the safe use of ICT throughout the school.

Signature……Date……..

Staff Professional Responsibilities

The HSCB eSafety subgroup group have produced a clear summary of **professional responsibilities related to the use of ICT** which has been endorsed by unions. To download visit http://www.thegrid.org.uk/eservices/safety/policies.shtml

PROFESSIONAL RESPONSIBILITIES

When using any form of ICT, including the Internet, in school and outside school

For your own protection we advise that you:

- Ensure all electronic communication with pupils, parents, carers, staff and others is compatible with your professional role and in line with school policies.
- Do not talk about your professional role in any capacity when using social media such as Facebook and YouTube.
- Do not put online any text, image, sound or video that could upset or offend any member of the whole school community or be incompatible with your professional role.
- Use school ICT systems and resources for all school business. This includes your school email address, school mobile phone and school video camera.
- Do not give out your own personal details, such as mobile phone number, personal e-mail address or social network details to pupils, parents, carers and others.
- Do not disclose any passwords and ensure that personal data (such as data held on MIS software) is kept secure and used appropriately.
- Only take images of pupils and/ or staff for professional purposes, in accordance with school policy and with the knowledge of SLT.
- Do not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.
- Ensure that your online activity, **both in school and outside school**, will not bring your organisation or professional role into disrepute.

You have a duty to report any eSafety incident which may impact on you, your professionalism or your organisation.

For HR support and guidance please contact 01438 844933
For eSafety support and guidance please contact 01438 844893

Computer Viruses

- All files downloaded from the Internet, received via e-mail or on removable media (e.g. floppy disk, CD, memory stick/pen drives) are checked for any viruses using the schools anti-virus software.

- Never interfere with any anti-virus software installed on school ICT equipment that you use

- If your machine is not routinely connected to the school network, you must make provision for regular virus updates through the Network team.

- You must log off your machine every night but leave powered on. This is to ensure that the scheduled operating system and antivirus updates are pushed to the school device to protect it.

- If you suspect there may be a virus on any school ICT equipment, stop using the equipment and contact your ICT support provider immediately. The ICT support provider will advise you what actions to take and be responsible for advising others that need to know

Data Security

The accessing and appropriate use of school data is something that the school takes very seriously.

The school follows Becta guidelines Becta Schools - Leadership and management - Security - Data handling security guidance for schools (published Spring 2009) and the Local Authority guidance documents listed below

HGfL: School Admin: School Office: Data Protection and Freedom of Information

- Headteacher's Guidance – Data Security in Schools – Dos and Don'ts

- Network Manager/MIS Administrator or Manager Guidance – Data Security in Schools

- SIRO/IAO Guidance – Data Security in Schools - Dos and Don'ts

Security

- The School gives relevant staff access to its Management Information System (SIMS), with a unique ID and password

- It is the responsibility of everyone to keep passwords secure

- Staff are aware of their responsibility when accessing school data

- Staff have been issued with the relevant guidance documents and the Policy for ICT Acceptable Use

- Staff have read the relevant guidance documents available on the SITSS website concerning 'Safe Handling of Data' (available on the grid at -

http://www.thegrid.org.uk/info/traded/sitss/)

- Staff keep all school related data secure. This includes all personal, sensitive, confidential or classified data.

- Staff should avoid leaving any portable or mobile ICT equipment or removable storage media in unattended vehicles. Where this is not possible, keep it locked out of sight

- Staff should always carry portable and mobile ICT equipment or removable media as hand luggage, and keep it under your control at all times

- It is the responsibility of individual staff to ensure the security of any personal, sensitive, confidential and classified information contained in documents faxed, copied, scanned or printed. This is particularly important when shared mopiers (multi-function print, fax, scan and copiers) are used

Anyone expecting a confidential/sensitive fax, should have warned the sender to notify before it is sent.

Impact Levels and Protective Marking

- Appropriate labelling of data should help schools secure data and so reduce the risk of security incidents
- Apply labelling in accordance with guidance from your Senior Information Risk Owner (SIRO)
- Most learner or staff personal data will be classed as Protect
- Protect and caveat classifications that schools may use are;

    - PROTECT – PERSONAL e.g. personal information about an individual
    - PROTECT – APPOINTMENTS e.g. to be used for information about visits from the Queen or government ministers
    - PROTECT – LOCSEN e.g. for local sensitive information
    - PROTECT – STAFF e.g. Organisational staff only
- Applying too high a protective marking can inhibit access, lead to unnecessary and expensive protective controls, and impair the efficiency of an organisation's business
- Applying too low a protective marking may lead to damaging consequences and compromise of the asset
- The sensitivity of an asset may change over time and it may be necessary to reclassify assets. If a document is being de-classified or the marking changed, the file should also be changed to reflect the highest marking within its contents

Reviews are continuing to look at the practical issues involved in applying protective markings to electronic and paper records and government representatives are working with suppliers to find ways of automatically marking reports and printouts.

Senior Information Risk Owner (SIRO)

The SIRO is a senior member of staff who is familiar with information risks and the school's response. Typically, the SIRO should be a member of the senior leadership team and have the following responsibilities:

- they own the information risk policy and risk assessment
- they appoint the Information Asset Owner(s) (IAOs)
- they act as an advocate for information risk management

The Office of Public Sector Information has produced *Managing Information Risk*, [http://www.nationalarchives.gov.uk/services/publications/information-risk.pdf] to support SIROs in their role.

The SIRO in this school is the Headteacher.

Information Asset Owner (IAO)

Any information that is sensitive needs to be protected. This will include the personal data of learners and staff; such as assessment records, medical information and special educational needs data. Barnwell School has identified several Information Asset Owners. For example, the school's Management Information System (MIS) should be identified as an asset and should have an Information Asset Owner. In this example the MIS Administrator or Manager could be the IAO. (See Authorised Staff Page 42)

The role of an IAO is to understand:

- what information is held, and for what purposes
- what information needs to be protected (e.g. any data that can be linked to an individual, student or staff etc including UPN, teacher DCSF number etc)
- how information will be amended or added to over time
- who has access to the data and why
- how information is retained and disposed off

As a result, the IAO is able to manage and address risks to the information and make sure that information handling complies with legal requirements. In a Secondary School, there may be several IAOs, whose roles may currently be those of e-safety coordinator, Network Manager or Management Information Systems administrator.

Although these roles have been explicitly identified, the handling of secured data is everyone's responsibility – whether they are an employee, consultant, software provider or managed service provider. Failing to apply appropriate controls to secure data could amount to gross misconduct or even legal action.

Disposal of Redundant ICT Equipment Policy

- All redundant ICT equipment will be disposed off through an authorised agency or via the Hertfordshire Business Services (HBS) disposal scheme. This should include a written receipt for the item including an acceptance of responsibility for the destruction of any personal data

- ICT equipment is ultimately the responsibility of the department the equipment belongs to (on departmental inventory); however advice and suggestions will be given by the Network Manager/Network Department.

- All redundant ICT equipment that may have held personal data will be irretrievably destroyed. We will only use authorised companies who will supply a written guarantee that this will happen.

- Disposal of any ICT equipment will conform to:

  The Waste Electrical and Electronic Equipment Regulations 2006
  The Waste Electrical and Electronic Equipment (Amendment) Regulations 2007
  http://www.environment-agency.gov.uk/business/topics/waste/32084.aspx
  http://www.opsi.gov.uk/si/si2006/uksi_20063289_en.pdf
  http://www.opsi.gov.uk/si/si2007/pdf/uksi_20073454_en.pdf?lang=_e
  Data Protection Act 1998
  http://www.ico.gov.uk/what_we_cover/data_protection.aspx
  Electricity at Work Regulations 1989
  http://www.opsi.gov.uk/si/si1989/Uksi_19890635_en_1.htm

- The school will maintain a comprehensive inventory of all its ICT equipment including a record of disposal

- The school's disposal record will include:

  - Date item disposed of
  - Authorisation for disposal, including:
    - verification of software licensing
    - any personal data likely to be held on the storage media?
  - How it was disposed of eg waste, gift, sale
  - Name of person & / or organisation who received the disposed item

* if personal data is likely to be held the storage media will be over written multiple times to ensure the data is irretrievably destroyed.

- Any redundant ICT equipment being considered for sale / gift will have been subject to a recent electrical safety check and hold a valid PAT certificate

Further information available at:

Waste Electrical and Electronic Equipment (WEEE) Regulations

Environment Agency web site

Introduction

http://www.environment-agency.gov.uk/business/topics/waste/32084.aspx

The Waste Electrical and Electronic Equipment Regulations 2006

http://www.opsi.gov.uk/si/si2006/uksi_20063289_en.pdf

The Waste Electrical and Electronic Equipment (Amendment) Regulations 2007

http://www.opsi.gov.uk/si/si2007/pdf/uksi_20073454_en.pdf?lang=_e

Information Commissioner website

http://www.ico.gov.uk/

Data Protection Act – data protection guide, including the 8 principles

http://www.ico.gov.uk/for_organisations/data_protection_guide.aspx

Data Protection Act – General Data Protection Regulation (GTPR)

https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/

PC Disposal – SITSS Information

http://www.thegrid.org.uk/info/traded/sitss/computers/pc_disposal.shtml

e-Mail

The use of e-mail within most schools is an essential means of communication for both staff and students. In the context of school, e-mail should not be considered private. Educationally, e-mail can offer significant benefits including; direct written contact between schools on different projects, be they staff based or student based, within school or international. We recognise that students need to understand how to style an e-mail in relation to their age and good network etiquette; 'netiquette'.

Managing e-Mail

- The school gives all staff their own e-mail account to use for all school business as a work-based tool This is to minimize the risk of receiving unsolicited or malicious e-mails and avoids the risk of personal profile information being revealed

- Staff & governors should use their school email for all professional communication

- It is the responsibility of each account holder to keep the password secure. For the safety and security of users and recipients, all mail is filtered and logged; if necessary, e-mail histories can be traced. The school email account should be the account that is used for all school business

- Under no circumstances should staff contact students, parents or conduct any school business using personal e-mail addresses

- All e-mails should be written and checked carefully before sending, in the same way as a letter written on school headed paper

- Staff sending e-mails to external organisations, parents or pupils, should cc their line manager when it is felt necessary in order to conduct their professional responsibilities.

- Students may only use school approved accounts on the school system and only for educational purposes

- E-mails created or received as part of your School job will be subject to disclosure in response to a request for information under the Freedom of Information Act 2000. You must therefore actively manage your e-mail account as follows:

  - Delete all e-mails of short-term value
  - Organise e-mail into folders and carry out frequent house-keeping on all folders and archives

- The following students have their own individual school issued accounts – Year 10, 11, 12 and 13, all other children use a class/ group e-mail address

- All student e-mail users are expected to adhere to the generally accepted rules of netiquette particularly in relation to the use of appropriate language and not revealing any personal details about themselves or others in e-mail communication, or arrange to meet anyone without specific permission, virus

checking attachments

- Students must immediately tell a teacher/ trusted adult if they receive an offensive e-mail and can report abuse through the school website using the CEOP.

- Staff must inform the eSafety co-ordinator and/or line manager if they receive an offensive e-mail

- Students are introduced to e-mail as part of the IT Scheme of Learning

- However, you access your school e-mail (whether directly, through webmail when away from the office or on non-school hardware) all the school e-mail policies apply

- The use of personal email accounts or any other Internet communication service for sending, reading or receiving business related e-mail is not permitted

Sending e-Mails

- If sending e-mails containing personal, confidential, classified or financially sensitive data to external third parties or agencies, refer to the Section e-mailing Personal, Sensitive, Confidential or Classified Information

- Use your own school e-mail account so that you are clearly identified as the originator of a message

- If you are required to send an e-mail from someone else's account, always sign on through the 'Delegation' facility within your e-mail software so that you are identified as the sender (if available within your software)

- Keep the number and relevance of e-mail recipients, particularly those being copied, to the minimum necessary and appropriate

- Do not send or forward attachments unnecessarily. Whenever possible, send the location path to the shared drive rather than sending attachments

- An outgoing e-mail greater than ten megabytes (including any attachments) is likely to be stopped automatically. This size limit also applies to incoming e-mail

- School e-mail is not to be used for personal use or advertising

Receiving e-Mails

- Check your e-mail regularly

- Activate your 'out-of-office' notification when away for extended periods. This may include advice on who to contact in your absence.

- Use the 'Delegation' facility within your e-mail software so that your e-mail can be handled by someone else while you are not at work (if available within your software)

- Never open emails, attachments, click on links from an untrusted or suspect source; Consult the Network Department.

- Do not use the e-mail systems to store attachments. Detach and save business related work to the appropriate shared drive/folder

- The automatic forwarding and deletion of e-mails is not allowed

- Users must not send emails which are offensive, embarrassing or upsetting to anyone (i.e. cyberbullying)

e-mailing Personal, Sensitive, Confidential or Classified Information

- Assess whether the information can be transmitted by other secure means before using e-mail - e-mailing confidential data is not recommended and should be avoided where possible
- Personal email accounts are not permitted for conducting school business. This also include personal, sensitive, confidential and classified information.

- Where your conclusion is that e-mail must be used to transmit such data:

  - Obtain express consent from your manager to provide the information by e-mail
  - Exercise caution when sending the e-mail and always follow these checks before releasing the e-mail:

    - Encrypt and password protect. See http://www.thegrid.org.uk/info/dataprotection/#securedata
    - Verify the details, including accurate e-mail address, of any intended recipient of the information
    - Verify (by phoning) the details of a requestor before responding to e-mail requests for information
    - Do not copy or forward the e-mail to any more recipients than is absolutely necessary

  - Do not send the information to anybody/person whose details you have been unable to separately verify (usually by phone)
  - Send the information as an encrypted document **attached** to an e-mail
  - Provide the encryption key or password by a **separate** contact with the recipient(s)
  - Do not identify such information in the subject line of any e-mail
  - Request confirmation of safe receipt

In exceptional circumstances, the County Council makes provision for secure data transfers to specific external agencies. Such arrangements are currently in place with:

  - Hertfordshire Constabulary

  - Hertfordshire Partnership Trust

Future Developments

The school includes a standard disclaimer to all staff external e-mail correspondence, stating that, 'the views expressed are not necessarily those of the school or the LA'.

When sending an e-mail containing personal or sensitive data you need to put a security classification in the first line of the e-mail. For e-mails to do with information about a student, for example, you need to put in **PROTECT – PERSONAL** on the first line of the e-mail.

This also needs to go on the top of any documents that you send (i.e. Word documents, Reports, Forms, including paper documents you send in hardcopy, etc). The name of the individual is not to be included in the subject line and the document containing the information encrypted. This provides additional security.

Equal Opportunities - Students with Additional Needs

The school endeavours to create a consistent message with parents for all students and this in turn should aid establishment and future development of the schools' eSafety rules.

However, staff are aware that some students may require additional teaching including reminders, prompts and further explanation to reinforce their existing knowledge and understanding of eSafety issues.

Where a student has poor social understanding, careful consideration is given to group interactions when raising awareness of eSafety. Internet activities are planned and well managed for these children and young people.

eSafety

eSafety - Roles and Responsibilities

As eSafety is an important aspect of strategic leadership within the school, the Head and governors have ultimate responsibility to ensure that the policy and practices are embedded and monitored. The school appoints an eSafety co-ordinator who has been designated this role by the Headteacher. All members of the school community have been made aware of who holds this post. It is the role of the eSafety co-ordinator to keep abreast of current issues and guidance through organisations such as Herts LA, Becta, CEOP (Child Exploitation and Online Protection) and Childnet.

Senior Management and Governors are updated by the Head/ eSafety co-ordinator and all governors have an understanding of the issues and strategies at our school in relation to local and national guidelines and advice.

This policy, supported by the school's acceptable use agreements for staff, governors, visitors and students, is to protect the interests and safety of the whole school community. It is linked to the following mandatory school policies: child protection, health and safety, home–school agreements, and behaviour/student discipline (including the anti-bullying) policy and PSHE

eSafety in the Curriculum

ICT and online resources are increasingly used across the curriculum. The school provides a comprehensive curriculum for online safety which enables pupils to become informed, safe and responsible. This includes teaching to prevent radicalisation, for which staff provide a narrative to counter extremism.

The curriculum is flexible and can respond to any immediate online safety issues and risks as they emerge.

It is necessary for pupils to develop skills of critical awareness, digital resilience and good online citizenship to enable them to use internet, mobile and digital technologies safely and responsibly. Pupils are taught to recognise the creative, collaborative, cultural, economic and educational opportunities provided by the internet, mobile and digital technologies.

Curriculum work will also include:

- Understanding how to use the internet, mobile and digital technologies in a balanced and appropriate way to avoid negative impact on wellbeing, e.g. regulated screen time and diverse online activity

- Learning how to develop a positive online reputation and enhance future opportunities e.g. in relationships and employment

- Developing critical thinking skills in relation to online content e.g. recognising fake news and extremism, understanding commercial manipulation, maintaining an authentic sense of self that is resilient to online pressure, learning how easy it is to lie online (i.e. users may not be who they say they are and may have ulterior motives)

- Understanding the dangers of giving out personal details online (e.g. full name,

address, mobile/home phone numbers, school details, IM/email address) and the importance of maintaining maximum privacy online

- Thinking carefully before placing images online and considering their appropriateness and understanding the importance of gaining consent before posting photographs of others

  Understanding the permanency of all online postings and conversations

- Understanding relevant legislation, including copyright, and the importance of respecting other people's information, reputation and images

- Students are aware of the impact of Cyberbullying and know how to seek help if they are affected by any form of online bullying. Students are also aware of where to seek advice or help if they experience problems when using the internet and related technologies; i.e. parent/ carer, teacher/ trusted staff member, or an organisation such as Childline or CEOP report abuse button

eSafety Skills Development for Staff

- Staff and governors are trained to fulfil their roles in online safety. The school audits the training needs of all school staff and provides regular training to improve their knowledge and expertise in the safe and appropriate use of internet, mobile and digital technologies. This training is recorded as part of safeguarding records

- New staff receive information on the school's acceptable use policy as part of their induction

- All staff will have been made aware of individual responsibilities relating to the safeguarding of children within the context of eSafety

- All staff are encouraged to incorporate eSafety activities and awareness within their curriculum areas

- All staff have been made aware of their individual responsibilities relating to the safeguarding of children within the context of eSafety and know what to do in the event of misuse of technology by any member of the school community (see eSafety Co-ordinator)

- All staff are encouraged to incorporate eSafety activities and awareness within their curriculum areas and ensure they are adequately informed with up-to-date areas of concern.

Managing the School eSafety Messages

- We endeavour to embed eSafety messages across the curriculum whenever the internet and/or related technologies are used

- The eSafety policy will be introduced to the students at the start of each school year

- eSafety posters will be prominently displayed
- The key eSafety advice will be promoted widely through school displays, newsletters, class activities and so on
    - We will participate in Safer Internet Day every February.

Visiting online sites and downloading

- Staff must preview sites, software and apps before their use in school or before recommending them to pupils. Before using any online service that requires user accounts to be created or the sharing of any personal data, staff must consult with the Data Protection Officer with details of the site/service. If internet research is set for homework, specific sites will be suggested that have previously been checked by the teacher. All users must observe copyright of materials from electronic sources.

- Staff must only use pre-approved systems if creating blogs, wikis or other online areas in order to communicate with pupils/ families.

- When working with pupils searching for images and other context, the school web filtering must ensure that it age appropriate.

Users must not:

Visit internet sites, make, post, download, upload or pass on, material, remarks, proposals or comments that contain or relate to:

- Indecent images of children actually or apparently under the age of 18 or images of child abuse (i.e. images of children, digital or cartoons, involved in sexual activity or posed to be sexually provocative)

- Indecent images of vulnerable people over the age of 18 (i.e. images of vulnerable people, digital or cartoons involved in sexual activity or posed to be sexually provocative)Adult material that breaches the Obscene Publications Act in the UK

- Promoting discrimination of any kind in relation to the protected characteristics: gender identity and reassignment, gender/sex, pregnancy and maternity, race, religion, sexual orientation, age and marital status

- Promoting hatred against any individual or group from the protected characteristics above

- Promoting illegal acts including physical or sexual abuse of children or adults, violence, bomb making, drug and alcohol abuse and software piracy

- Any material that may bring the school or any individual within it into disrepute e.g. promotion of violence, gambling, libel and disrespect

Users must not:

- Reveal or publicise confidential or proprietary information

- Intentionally interfere with the normal operation of the internet connection, including the propagation of computer viruses

- Transmit unsolicited commercial or advertising material either to other users, or to organisations connected to other networks except where permission has been given to the school

- Use the school's hardware and Wi-Fi facilities for running a private business

- Intimidate, threaten or cause harm to others

- Access or interfere in any way with other users' accounts

- Use software or hardware that has been prohibited by the school

Personal devices may be used to conduct school business outside of school using the school's authorised and secured Cloud Systems but access to the personal device must secured (using a PIN, biometric or password) and cannot be in breach of GTPR by holding personal data on such devices. .

All breaches of prohibited behaviours detailed above will be investigated, where appropriate, in liaison with the police.

The school recognises that in certain planned curricular activities, access to controversial and/or offensive online content may be beneficial for educational use. In such circumstances, there is an expectation that access is pre-planned, risk assessed and recorded, and permission given by Executive Headteacher or Head of School..

Incident Reporting, eSafety Incident Log & Infringements

Incident Reporting

Any security breaches or attempts, loss of equipment and any unauthorised use or suspected misuse of ICT must be immediately reported to the school's SIRO or eSafety Co-ordinator. Additionally, all security breaches, lost/stolen equipment or data, virus notifications, unsolicited emails, misuse or unauthorised use of ICT and all other policy non-compliance must be reported to your eSafety Co-ordinator.

eSafety Incident Log

Some incidents may need to be recorded in other places, such as Solero, if they relate to a bullying or racist incident.

Barnwell School eSafety Incident Log

Details of ALL eSafety incidents to be recorded by the eSafety Coordinator. This incident log will be monitored termly by the Headteacher, Member of SLT or Chair of Governors. Any incidents involving Cyberbullying should be recorded on the 'Integrated Bullying and racist Incident Record Form 2'

Date & time	Name of pupil or staff member	Male or Female	Room and computer/ device number	Details of incident (including evidence)	Actions and reasons

Misuse and Infringements

Complaints

Complaints and/ or issues relating to eSafety should be made to the eSafety co-ordinator or Headteacher. Incidents should be logged and the **Hertfordshire Flowcharts for Managing an eSafety Incident** should be followed.

Inappropriate Material

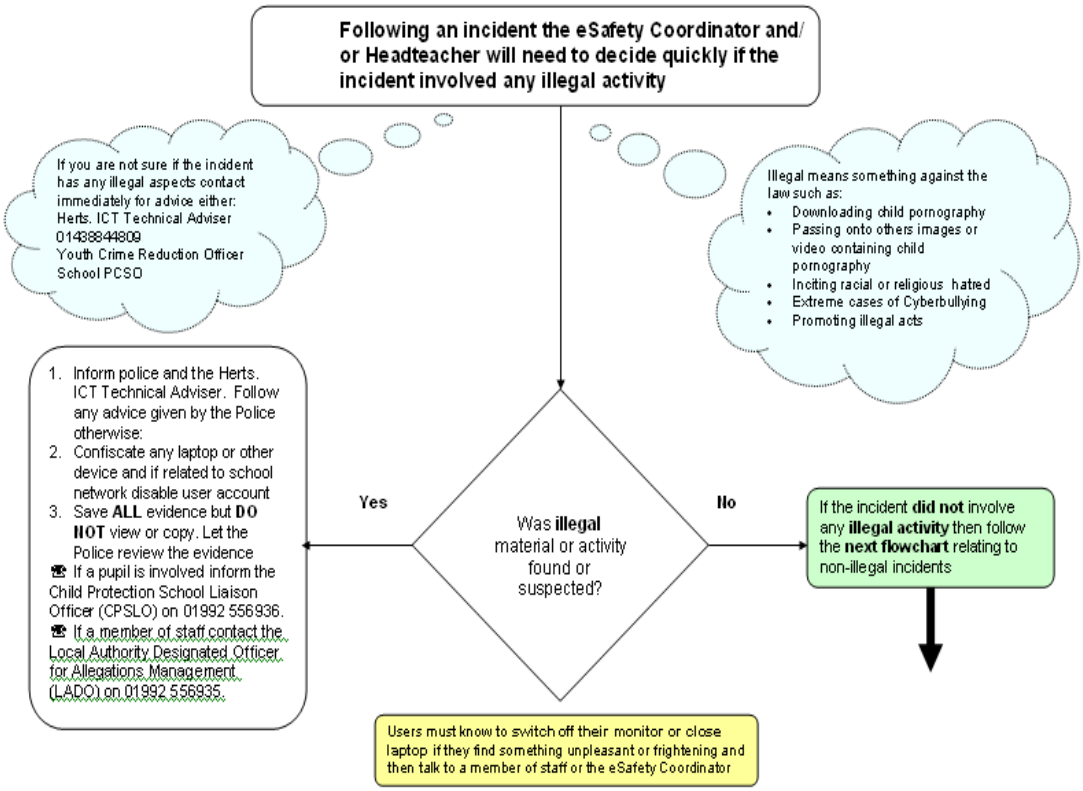
- All users are aware of the procedures for reporting accidental access to inappropriate materials. The breach must be immediately reported to the eSafety co-ordinator
- Deliberate access to inappropriate materials by any user will lead to the incident being logged by the eSafety co-ordinator, depending on the seriousness of the offence; investigation by the Headteacher/ LA, immediate suspension, possibly leading to dismissal and involvement of police for very serious offences (see flowchart)
- Users are made aware of sanctions relating to the misuse or misconduct by reading and signing the Acceptable Use Agreement.

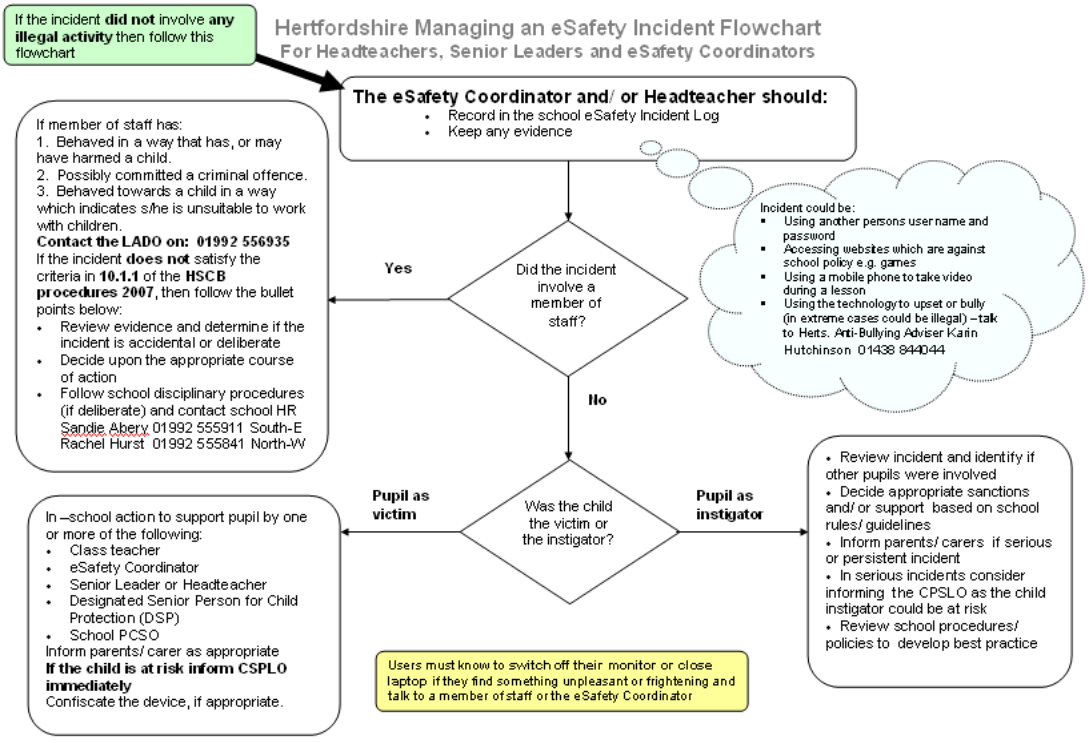
Flowcharts for Managing an eSafety Incident

http://www.thegrid.org.uk/eservices/safety/research/incident.shtml)

Hertfordshire Flowchart to support decisions related to an Illegal eSafety Incident

For Headteachers, Senior Leaders and eSafety Coordinators





Reporting incidents, abuse and inappropriate material
There may be occasions in school when either a pupil or an adult receives an offensive, abusive or inappropriate message or accidentally accesses upsetting or abusive material. When such a situation occurs the pupil or adult must report the incident immediately to the first available member of staff, the DSL, the Head of School. Where such an incident may lead to significant harm, safeguarding procedures should be followed. The school takes the reporting of such incidents seriously and where judged necessary, the DSL will refer details to social care or the police.

Internet Access

The internet is an open communication medium, available to all, at all times. Anyone can view information, send messages, discuss ideas and publish material which makes it both an invaluable resource for education, business and social interaction, as well as a potential risk to young and vulnerable people. All use of the **Hertfordshire Grid for Learning** (HGfL) is logged and the logs are randomly but regularly monitored. Whenever any inappropriate use is detected it will be followed up.

Managing the Internet

- Students will have supervised access to Internet resources (where reasonable) through the school's fixed and mobile internet technology
- Staff will preview any recommended sites before use
- Raw image searches are discouraged when working with students
- If Internet research is set for homework, specific sites will be suggested that have previously been checked by the teacher. It is advised that parents recheck these sites and supervise this work. Parents will be advised to supervise any further research
- All users must observe software copyright at all times. It is illegal to copy or distribute school software or illegal software from other sources
- All users must observe copyright of materials from electronic resources

Internet Use

- You must not post personal, sensitive, confidential or classified information or disseminate such information in any way that may compromise its intended restricted audience
- Don't reveal names of colleagues, students, governors, clients or any other confidential information acquired through school on any social networking site or blog
- On-line gambling is not allowed
- On-line gaming is not allowed

- Online shopping is not allowed
- All inappropriate adult entertainment is not allowed

It is at the Headteacher's discretion on what internet activities are permissible for staff and students and how this is disseminated.

Infrastructure

- Hertfordshire Local Authority has a monitoring solution via the Hertfordshire Grid for Learning where web-based activity is monitored and recorded
- School internet access is controlled through the LA's web filtering service. For further information relating to filtering please go to http://www.thegrid.org.uk/eservices/safety/filtered.shtml
- Barnwell School also employs some additional web filtering which is the responsibility of the Network Department.
- Barnwell School is aware of its responsibility when monitoring staff communication under current legislation and takes into account; Data Protection Act 1998, The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, Regulation of Investigatory Powers Act 2000, Human Rights Act 1998
- Staff and students are aware that school based email and internet activity can be monitored and explored further if required
- The school does not allow students access to internet logs
- The school uses management control tools for controlling and monitoring workstations
- If staff or students discover an unsuitable site, the screen must be switched off/ closed and the incident reported immediately to the e-safety coordinator or teacher as appropriate
- It is the responsibility of the school, by delegation to the network manager, to ensure that Anti-virus protection is installed and kept up-to-date on all school machines
- Students and Staff using personal removable media are responsible for measures to protect against viruses, for example making sure that additional systems used have up-to-date virus protection software. It is not the school's responsibility to install or maintain virus protection on personal systems.
- Students and staff are not permitted to download programs or files on school based technologies without seeking prior permission from the Network department
- If there are any issues related to viruses or anti-virus software, the network manager should be informed via email or in person.

Managing Other Technologies

Social networking sites and other online internet communication services such as Twitter; Facebook and Skype etc, if used responsibly both outside and within an educational context can provide easy to use, creative, collaborative and free facilities. However, it is important to recognise that there are issues regarding the appropriateness of some content, contact, culture and commercialism. To this end, we encourage our students to think carefully about the way that information can be added and removed by all users, including themselves, from these sites.

- At present, the school endeavors to deny access to social networking sites to students within school
- All students are advised to be cautious about the information given by others on sites, for example users not being who they say they are
- Students are taught to avoid placing images of themselves (or details within images that could give background details) on such sites and to consider the appropriateness of any images they post due to the difficulty of removing an image once online
- Students are always reminded to avoid giving out personal details on such sites which may identify them or where they are (full name, address, mobile/ home phone numbers, school details, IM/ email address, specific hobbies/ interests)
- Our students are advised to set and maintain profiles on such sites to maximum privacy and deny access to unknown individuals
- Students are encouraged to be wary about publishing specific and detailed private thoughts online
- Our students are asked to report any incidents of bullying to the school
- Staff may only create blogs, wikis or other social networking/internet communication services to communicate with students with the approval of the Headteacher

Parental Involvement

We believe that it is essential for parents/ carers to be fully involved with promoting eSafety both in and outside of school and also to be aware of their responsibilities. We regularly consult and discuss eSafety with parents/ carers and seek to promote a wide understanding of the benefits related to ICT and associated risks.

- Parents/carers are required to make a decision as to whether they consent to images of their child being taken/ used in the public domain (e.g. on school website)

- Parents/carers are asked to read through and sign the Acceptable Use Agreement containing the following statement

    - We will support the school approach to on-line safety and not deliberately upload or add any images, sounds or text that could upset or offend any member of the school community

- The school disseminates information to parents relating to eSafety where appropriate in the form of;

    - Information evenings
    - Posters
    - School website information
    - Newsletter items

Passwords and Password Security

Passwords

Please refer to the document on the grid for guidance on How to Encrypt Files which contains guidance on creating strong passwords and password security

http://www.thegrid.org.uk/info/dataprotection/index.shtml#securedata

- **Always use your own** personal passwords to access computer based services
- Make sure you enter your personal passwords each time you logon. Do not include passwords in any automated logon procedures
- Staff should change temporary passwords at first logon
- Change passwords whenever there is any indication of possible system or password compromise
- Do not record passwords or encryption keys on paper or in an unprotected file
- Only disclose your personal password to authorised ICT support staff when necessary, and never to anyone else. Ensure that all personal passwords that have been disclosed are changed once the requirement is finished
- User ID and passwords for staff and students who have left the School are removed from the system within 2 weeks.
- Never tell a child or colleague your password

If you think your password may have been compromised or someone else has become aware of your password report this to the Network team

Password Security
Password security is essential for staff, particularly as they are able to access and use student data. Staff are expected to have secure passwords which are not shared with

anyone. The students are expected to keep their passwords secret and not to share with others, particularly their friends. Staff and students are regularly reminded of the need for password security.

- All users read and sign an Acceptable Use Agreement to demonstrate that they have understood the school's e-safety Policy and Data Security
- Users are provided with an individual network, email and SIMS log-in username.
- Students are not allowed to deliberately access on-line materials or files on the school network, of their peers, teachers or others
- Staff are aware of their individual responsibilities to protect the security and confidentiality of school networks and MIS systems, including ensuring that passwords are not shared and are changed periodically. Individual staff users must also make sure that workstations are not left unattended and are locked.
- In our school, all ICT password policies are the responsibility of the Network Manager and all staff and students are expected to comply with the policies at all times

Zombie Accounts

Zombie accounts refers to accounts belonging to users who have left the school and therefore no longer have authorised access to the school's systems. Such Zombie accounts when left active can cause a security threat by allowing unauthorised access.

- Ensure that all user accounts are disabled once the member of the school has left
- Prompt action on disabling accounts will prevent unauthorized access
- Regularly change generic passwords to avoid unauthorized access

Further advice available http://www.itgovernance.co.uk/

Personal or Sensitive Information

Protecting Personal, Sensitive, Confidential and Classified Information

- Ensure that any School information accessed from your own PC or removable media equipment is kept secure
- Ensure you lock your screen before moving away from your computer during your normal working day to prevent unauthorised access
- Ensure the accuracy of any personal, sensitive, confidential and classified information you disclose or share with others
- Ensure that personal, sensitive, confidential or classified information is not disclosed to any unauthorised person
- Ensure the security of any personal, sensitive, confidential and classified

information contained in documents you fax, copy, scan or print. This is particularly important when shared mopiers (multi-function print, fax, scan and copiers) are used and when access is from a non-school environment

- Only download personal data from systems if expressly authorised to do so by your manager

- You must not post on the internet personal, sensitive, confidential, or classified information, or disseminate such information in any way that may compromise its intended restricted audience

- Keep your screen display out of direct view of any third parties when you are accessing personal, sensitive, confidential or classified information

- Ensure hard copies of data are securely stored and disposed of after use in accordance with the document labeling

Storing/Transferring Personal, Sensitive, Confidential or Classified Information Using Removable Media

- Store all removable media securely; consider encryption if appropriate

- Securely dispose of removable media that may hold personal data

- Ensure hard drives from machines no longer in service are removed and stored securely or wiped clean

- Removable media can be subjected to security checks.

Digital continuity

- Computerised data that must be kept for six or more years will be identified, and stored appropriately:
- This data will be stored in online and cloud backup systems.
- The data will be archived to a dedicated location on the school's server, which is password-protected
- This data will be stored on password protected external hard drives.]
- This data will not be stored on flash drives.
- Where possible, files will be converted to appropriate supported file formats for long-term preservation e.g. Word and Excel files may be converted to PDF files.

Safe Use of Images

Taking of Images and Film

Digital images are easy to capture, reproduce and publish and, therefore, misuse. We must remember that it is not always appropriate to take or store images of any member of the school community or public, without first seeking consent and considering the appropriateness.

- Parents/carers are regularly offered the option of withdrawing permission for the school to take images of their child for school purposes only. Parents/carers should write to the school expressing their wish for their child not to be

photographed/filmed.

- The school permits the appropriate taking of images of staff and students by staff and students with school equipment; unless withdrawal of permission has been received.

- Staff are not permitted to use personal digital equipment, such as mobile phones and cameras, to record images of students, this includes when on field trips. However, with the express permission of the Headteacher, images can be taken provided they are transferred immediately and solely to the school's network and deleted from the staff device

- Students are not permitted to use personal digital equipment, including mobile phones and cameras, to record images of the others, this includes when on field trips. However, with the express permission of the Headteacher, images can be taken provided they are transferred immediately and solely to the school's network and deleted from the student's device

Publishing Student's Images and Work

On a child's entry to the school, all parents/carers will be asked to give permission to use their child's work/photos in the following ways:

- on the school web site

- in the school prospectus and other printed publications that the school may produce for promotional purposes

- recorded/ transmitted on a video or webcam

- in display material that may be used in the school's communal areas

- in display material that may be used in external areas, ie exhibition promoting the school

- general media appearances, eg local/ national media/ press releases sent to the press highlighting an activity (sent using traditional methods or electronically)

This consent form is considered valid for the entire period that the child attends this school unless there is a change in the child's circumstances where consent could be an issue, eg divorce of parents, custody issues, etc.

Parents/ carers may withdraw permission, in writing, at any time.

Students' names will not be published alongside their image and vice versa. E-mail and postal addresses of students will not be published. Students' full names will not be published.

Before posting student work on the Internet, a check needs to be made to ensure that permission has been given for work to be displayed.

Only the Web Administrator has authority to upload to the site.

For further information relating to issues associated with School websites and the safe use of images in Hertfordshire schools, see

http://www.thegrid.org.uk/schoolweb/safety/index.shtml
http://www.thegrid.org.uk/info/csf/policies/index.shtml#images

Storage of Images

- Photographs and videos provide valuable evidence of pupils' achievement and progress in a variety of contexts and can be used to celebrate the work of the school. In line with GDPR they are used only with the written consent of parents/carers which is secured in the first instance on a child's entry to the school. Records are kept on file and consent can be changed by parents/carers at any time. (See GDPR policy for greater clarification).

- Photographs and images of pupils are only stored on the school's agreed secure networks which include some cloud based services. Staff and pupils may have access to photographs taken during a class session, but these will be transferred/deleted promptly.

- Parents/carers should note that there may be some children who are at risk and must not have their image put online and others who do not want their image online. For these reasons parents/carers must follow the school's Acceptable Use Agreement and refrain from taking or posting online photographs of any member of the school community, other than their own child/ren.

  - Staff and other professionals working with pupils, must only use school equipment to record images of pupils whether on or off site. See also GDPR. Permission to use images of all staff who work at the school is sought on induction and a written record is located in the personnel file
  - Images/ films of children are stored on the school's network.

  - Students and staff are not permitted to use personal portable media for storage of images (e.g., USB sticks) without the express permission of the Headteacher

  - Rights of access to this material are restricted to the teaching staff and students within the confines of the school network.

  - Each Head of Department has the responsibility of deleting the images when they are no longer required, or the student has left the school

Webcams and CCTV

- The school uses CCTV for security and safety. The only person with access to this is the Senior Information Officer/Site Manager. Notification of CCTV use is displayed at the front of the school. Please refer to the hyperlink below for further guidance http://www.ico.gov.uk/for_organisations/topic_specific_guides/cctv.aspx

- We do not use publicly accessible webcams in school

- Webcams in school are only ever used for specific learning purposes, i.e. monitoring hens' eggs and never using images of children or adults

- Misuse of the webcam by any member of the school community will result in sanctions (as listed under the 'inappropriate materials' section of this document)

For further information relating to webcams and CCTV, please see http://www.thegrid.org.uk/schoolweb/safety/webcams.shtml

Video Conferencing

- Permission is sought from parents and carers if their children are involved in video conferences

- Permission is sought from parents and carers if their children are involved in video conferences with end-points outside of the school

- All students are supervised by a member of staff when video conferencing

- All students are supervised by a member of staff when video conferencing with end-points beyond the school

- Approval from the Headteacher is sought prior to all video conferences within school

- The school conferencing equipment is not set to auto-answer and is only switched on for scheduled and approved conferences

- No part of any video conference is recorded in any medium without the written consent of those taking part

Additional points to consider:

- Participants in conferences offered by 3rd party organisations may not be CRB checked

- Conference supervisors need to be familiar with how to use the video conferencing equipment, particularly how to end a call if at any point any person taking part becomes unhappy with the content of the conference

For further information and guidance relating to Video Conferencing, please see **http://www.thegrid.org.uk/learning/ict/technologies/videoconferencing/index.shtml**

School ICT Equipment including Portable & Mobile ICT Equipment & Removable Media

School ICT Equipment

- As a user of ICT, you are responsible for any activity undertaken on the school's ICT equipment provided to you

- It is recommended that schools log ICT equipment issued to staff and record serial numbers as part of the school's inventory

- Do not allow your visitors to plug their ICT hardware into the school network points (unless special provision has been made). They should use the school's wireless guest facility.

- Ensure that all ICT equipment that you use is kept physically secure

- Do not attempt unauthorised access or make unauthorised modifications to computer equipment, programs, files or data. This is an offence under the Computer Misuse Act 1990

- It is imperative that you save your data on a frequent basis to the school's network drive. You are responsible for the backup and restoration of any of your data that is not held on the school's network drive

- Personal or sensitive data should not be stored on the local drives of desktop PCs. If it is necessary to do so the local drive must be encrypted

- A time locking screensaver is applied to all machines.

- Privately owned ICT equipment should not be used on a school network other than the Wireless BYOD networks

- On termination of employment, resignation or transfer, return all ICT equipment to your Manager. You must also provide details of all your system logons so that they can be disabled

- It is your responsibility to ensure that any information accessed from your own PC or removable media equipment is kept secure, and that no personal, sensitive, confidential or classified information is disclosed to any unauthorised person

- All ICT equipment allocated to staff must be authorised by the appropriate Line Manager. Authorising Managers are responsible for:

    - maintaining control of the allocation and transfer within their Unit
    - recovering and returning equipment when no longer needed

- All redundant ICT equipment is disposed of in accordance with Waste Electrical and Electronic Equipment (WEEE) directive and Data Protection Act (DPA)

Portable & Mobile ICT Equipment

This section covers such items as laptops, PDAs and removable data storage devices. Please refer to the relevant sections of this document when considering storing or transferring personal or sensitive data

- All activities carried out on School systems and hardware will be monitored in accordance with the general policy

- Staff must ensure that all school data is stored on school's network, and not

kept solely on the laptop. Any equipment where personal data is likely to be stored must be encrypted

- Equipment must be kept physically secure in accordance with this policy to be covered for insurance purposes. When travelling by car, best practice is to place the laptop in the boot of your car before starting your journey

- Synchronise all locally stored data, including diary entries, with the central school network server on a frequent basis

- Ensure portable and mobile ICT equipment is made available as necessary for anti-virus updates and software installations, patches or upgrades

- The installation of any applications or software packages must be authorised by the ICT support team, fully licensed and only carried out by your ICT support

- In areas where there are likely to be members of the general public, portable or mobile ICT equipment must not be left unattended and, wherever possible, must be kept out of sight

- Portable equipment must be transported in its protective case if supplied

New Technologies Devices

New personal technologies offer new opportunities for teaching and learning including a move towards personalised learning and 1:1 device ownership for children and young people. Many existing mobile technologies such as portable media players, PDAs, gaming devices, mobile and Smart phones are familiar to children outside of school too. They often provide a collaborative, well-known device with possible internet access and thus open up risk and misuse associated with communication and internet use. New technologies will be examined for educational benefit and the risk assessed before use in school is allowed. Barnwell School chooses to manage the use of these devices in the following ways so that users exploit them appropriately.

Personal Mobile Devices (including phones)

- The school allows staff to bring in personal mobile phones and devices for their own use. Under no circumstances does the school allow a member of staff to contact a student or parent/ carer using their personal device or personal accounts

- Students are allowed to bring personal mobile devices/phones to school but must not use them for personal purposes. At all times the device must be switched onto silent

- The school is not responsible for the loss, damage or theft of any personal mobile device

- The sending of inappropriate text messages and/or media between any member of the school community is not allowed

- Permission must be sought before any image or sound recordings are made on

these devices of any member of the school community

- Users bringing personal devices into school must ensure there is no inappropriate or illegal content on the device

- If a student is seen to be using their mobile device/phone and it is believed the content may be used for inappropriate activities a member of the Senior Leadership Team has the right to view the content of the phone.

School Provided Mobile Devices (including phones)

- The sending of inappropriate text messages/other communication methods between any member of the school community is not allowed

- Permission must be sought before any image or sound recordings are made on the devices of any member of the school community

- Where the school provides mobile technologies such as phones, laptops and PDAs for offsite visits and trips, only these devices should be used

- Where the school provides a laptop for staff, only this device may be used to conduct school business outside of school

Removable Media

If storing/transferring personal, sensitive, confidential or classified information using Removable Media please refer to the section 'Storing/Transferring Personal, Sensitive, Confidential or Classified Information Using Removable Media'

- Only use recommended removable media
- Store all removable media securely
- Removable media must be disposed of securely by your ICT support team

Servers

- Always keep servers in a locked and secure environment

- Limit access rights

- Always password protect and lock the server

- Existing servers should have security software installed appropriate to the machine's specification

- Data must be backed up regularly

- Remote (Cloud) back ups should be automatically securely encrypted.

Smile and Stay Safe Poster

eSafety guidelines to be displayed throughout the school

MILE and stay safe

Staying safe means keeping your personal details private, such as full name, phone number, home address, photos or school. Never reply to ASL (age, sex, location)

Meeting up with someone you have met online can be dangerous. Only meet up if you have first told your parent or carer and they can be with you.

Information online can be untrue, biased or just inaccurate. Someone online my not be telling the truth about who they are - they may not be a 'friend'

Let a parent, carer, teacher or trusted adult know if you ever feel worried, uncomfortable or frightened about something online or someone you have met or who has contacted you online.

Emails, downloads, IM messages, photos and anything from someone you do not know or trust may contain a virus or unpleasant message. So do not open or reply.

Systems and Access

- You are responsible for all activity on school systems carried out under any access/account rights assigned to you, whether accessed via school ICT equipment or your own PC

- Do not allow any unauthorised person to use school ICT facilities and services that have been provided to you

- Use only your own personal logons, account IDs and passwords and do not allow them to be used by anyone else

- Keep your screen display out of direct view of any third parties when you are accessing personal, sensitive, confidential or classified information

- Ensure you lock your screen before moving away from your computer during your normal working day to protect any personal, sensitive, confidential or otherwise classified data and to prevent unauthorised access

- Ensure that you logoff from the PC completely when you are going to be away from the computer for a longer period of time

- Do not introduce or propagate viruses

- It is imperative that you do not access, load, store, post or send from school ICT any material that is, or may be considered to be, illegal, offensive, libellous, pornographic, obscene, defamatory, intimidating, misleading or disruptive to the school or may bring the school or HCC into disrepute. This includes, but is not limited to, jokes, chain letters, files, emails, clips or images that are not part of the school's business activities; sexual comments or images, nudity, racial slurs, gender specific comments, or anything that would offend someone on the basis of their age, sexual orientation, religious or political beliefs, national origin, or disability (in accordance with the Sex Discrimination Act, the Race Relations Act and the Disability Discrimination Act)

- Any information held on School systems, hardware or used in relation to School business may be subject to The Freedom of Information Act

- Where necessary, obtain permission from the owner or owning authority and pay any relevant fees before using, copying or distributing any material that is protected under the Copyright, Designs and Patents Act 1998

- It is essential that any hard drives which may have held personal or confidential data are 'scrubbed' in way that means the data can no longer be read. It is not sufficient to simply delete the files or reformat the hard drive. Whoever you appoint to dispose of the equipment must provide a **written guarantee** that they will irretrievably destroy the data by multiple over writing the data.

Telephone Services

- You may make or receive personal telephone calls provided:

    1. They are infrequent, kept as brief as possible and do not cause annoyance to others

    2. They are not for profit or to premium rate services

    3. They conform to this and other relevant HCC and school policies.

- School telephones are provided specifically for school business purposes and personal usage is a privilege that will be withdrawn if abused

- Be aware that the laws of slander apply to telephone calls. Whilst a telephone call may seem to have a temporary and private existence it still qualifies as admissible evidence in slander law cases

- Ensure that your incoming telephone calls can be handled at all times

Mobile Phones

- There is a school mobile phone for the purposes of school trips only.

- The trip organizer or other appropriate adult is responsible for the security of the school mobile phone. Do not leave it unattended and on display (especially in vehicles)

- Report the loss or theft of any school mobile phone equipment immediately

- The school remains responsible for all call costs until the phone is reported lost or stolen

- You must read and understand the user instructions and safety points relating to the use of your school mobile phone prior to using it

- School SIM cards must only be used in school provided mobile phones

- All school mobile phones are barred from calling premium rate numbers and any numbers outside of the UK as the default

- You must not send text messages to premium rate services

- Never use a hand-held mobile phone whilst driving a vehicle. Only genuine 999 or 112 emergency calls may be made if it would be unsafe to stop before doing so

Social Media, including Facebook and Twitter

Facebook, Twitter and other forms of social media are increasingly becoming an important part of our daily lives.

- Barnwell School uses Facebook and Twitter to communicate with parents and

carers. The Deputy Headteachers are responsible for all postings on these technologies and monitors responses from others

- Staff *are* permitted to access their personal social media accounts (if not interfering with their daily work and as an exception rather than the norm) using school equipment at

- Staff are able to setup Social Learning Platform accounts, using their school email address, in order to be able to teach pupils the safe and responsible use of Social Media

- Students are not permitted to access their social media accounts whilst at school

- Staff, governors, pupils, parents and carers are regularly provided with information on how to use social media responsibly and what to do if they are aware of inappropriate use by others

- Staff, governors, pupils, parents and carers are aware that the information, comments, images and video they post online can be viewed by others, copied and stay online forever

- Staff, governors, pupils, parents and carers are aware that their online behaviour should at all times be compatible with UK law

Writing and Reviewing this Policy

Staff Involvement in Policy Creation

- Staff involved in making/ reviewing the Policy for ICT Acceptable Use as follows:

eSafety Coordinator
Network Manager
Headteacher
Environment Committee – School Governors

Review Procedure

There will be an on-going opportunity for staff to discuss with the eSafety coordinator any issue of eSafety that concerns them

There will be an on-going opportunity for staff to discuss with the SIRO/AIO any issue of data security that concerns them

This policy will be reviewed every (24) months and consideration given to the implications for future whole school development planning

The policy will be amended if new technologies are adopted or Central Government change the orders or guidance in any way

Authorised Staff

ICT Authorised Staff – as mentioned in *Monitoring* and throughout.

Head teacher (Executive and Head of Schools)

Network Technicians

Asset Information Owner – A.I.O.

Senior Information Owner – S.I.R.O.

Current Legislation

Acts Relating to Monitoring of Staff eMail

Data Protection Act 1998

The Act requires anyone who handles personal information to comply with important data protection principles when treating personal data relating to any living individual. The Act grants individuals rights of access to their personal data, compensation and prevention of processing.

http://www.legislation.gov.uk/ukpga/1998/29/contents

The Telecommunications (Lawful Business Practice)

(Interception of Communications) Regulations 2000

http://www.legislation.gov.uk/uksi/2000/2699/contents/made (updated Link)

Regulation of Investigatory Powers Act 2000

Regulating the interception of communications and making it an offence to intercept or monitor communications without the consent of the parties involved in the communication. The RIP was enacted to comply with the Human Rights Act 1998. The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, however, permit a degree of monitoring and record keeping, for example, to ensure communications are relevant to school activity or to investigate or detect unauthorised use of the network. Nevertheless, any monitoring is subject to informed consent, which means steps must have been taken to ensure that everyone who may use the system is informed that communications may be monitored. Covert monitoring without informing users that surveillance is taking place risks breaching data protection and privacy legislation.

http://www.hmso.gov.uk/acts/acts2000/20000023.htm

Human Rights Act 1998

http://www.hmso.gov.uk/acts/acts1998/19980042.htm

Other Acts Relating to eSafety

Racial and Religious Hatred Act 2006

It a criminal offence to threaten people because of their faith, or to stir up religious hatred by displaying, publishing or distributing written material which is threatening. Other laws already protect people from threats based on their race, nationality or ethnic

background.

Sexual Offences Act 2003

The new grooming offence is committed if you are over 18 and have communicated with a child under 16 at least twice (including by phone or using the Internet) it is an offence to meet them or travel to meet them anywhere in the world with the intention of committing a sexual offence. Causing a child under 16 to watch a sexual act is illegal, including looking at images such as videos, photos or webcams, for your own gratification. It is also an offence for a person in a position of trust to engage in sexual activity with any person under 18, with whom they are in a position of trust. Schools should already have a copy of "*Children & Families: Safer from Sexual Crime*" document as part of their child protection packs.

For more information www.teachernet.gov.uk

Communications Act 2003 (section 127)

Sending by means of the Internet a message or other matter that is grossly offensive or of an indecent, obscene or menacing character; or sending a false message by means of or persistently making use of the Internet for the purpose of causing annoyance, inconvenience or needless anxiety is guilty of an offence liable, on conviction, to imprisonment. This wording is important because an offence is complete as soon as the message has been sent: there is no need to prove any intent or purpose.

The Computer Misuse Act 1990 (sections 1 – 3)

Regardless of an individual's motivation, the Act makes it a criminal offence to gain:

- access to computer files or software without permission (for example using another persons password to access files)
- unauthorised access, as above, in order to commit a further criminal act (such as fraud)
- impair the operation of a computer or program

UK citizens or residents may be extradited to another country if they are suspected of committing any of the above offences.

Malicious Communications Act 1988 (section 1)

This legislation makes it a criminal offence to send an electronic message (e-mail) that conveys indecent, grossly offensive, threatening material or information that is false; or is of an indecent or grossly offensive nature if the purpose was to cause a recipient to suffer distress or anxiety.

Copyright, Design and Patents Act 1988

Copyright is the right to prevent others from copying or using work without permission. Works such as text, music, sound, film and programs all qualify for copyright protection. The author of the work is usually the copyright owner, but if it was created during the course of employment it belongs to the employer. Copyright infringement is to copy all or a substantial part of anyone's work without obtaining them author's permission.

Usually a licence associated with the work will allow a user to copy or use it for limited purposes. It is advisable always to read the terms of a licence before you copy or use someone else's material. It is also illegal to adapt or use software without a licence or in ways prohibited by the terms of the software licence.

Public Order Act 1986 (sections 17 – 29)

This Act makes it a criminal offence to stir up racial hatred by displaying, publishing or distributing written material which is threatening. Like the Racial and Religious Hatred Act 2006 it also makes the possession of inflammatory material with a view of releasing it a criminal offence.

Protection of Children Act 1978 (Section 1)

It is an offence to take, permit to be taken, make, possess, show, distribute or advertise indecent images of children in the United Kingdom. A child for these purposes is a anyone under the age of 18. Viewing an indecent image of a child on your computer means that you have made a digital image. An image of a child also covers pseudo-photographs (digitally collated or otherwise). A person convicted of such an offence may face up to 10 years in prison.

Obscene Publications Act 1959 and 1964

Publishing an "obscene" article is a criminal offence. Publishing includes electronic transmission.

Protection from Harassment Act 1997

A person must not pursue a course of conduct, which amounts to harassment of another, and which he knows or ought to know amounts to harassment of the other.

A person whose course of conduct causes another to fear, on at least two occasions, that violence will be used against him is guilty of an offence if he knows or ought to know that his course of conduct will cause the other so to fear on each of those occasions.

Acts Relating to the Protection of Personal Data

Data Protection Act 1998

http://www.opsi.gov.uk/acts/acts1998/ukpga_19980029_en_1

The Freedom of Information Act 2000

http://www.ico.gov.uk/for_organisations/freedom_of_information_guide.aspx

---

Counter-Terrorism and Security Act 2015 (Prevent), Anti-Radicalisation & Counter-Extremism Guidance

https://www.gov.uk/government/publications/preventing-extremism-in-schools-and-childrens-services