Cavendish
Primary School

E-Safety Policy

Safeguarding pupils,

staff and the school in a digital world

Table of Contents

Acknowledgement

This document is based on an original document 'YHGfL Guidance for creating an E-Safety Policy' produced by the YHGfL E-Safety Officer and adapted by Cavendish Primary School.

Introduction

This E-Safety policy recognises our commitment to E-Safety and acknowledges its part in the school's overall Safeguarding policies and procedures. It shows our commitment to meeting the requirements to keep pupils safe in the 'Every Child Matters' agenda.

We believe the whole school community can benefit from the opportunities provided by the Internet and other technologies used in everyday life. The E-Safety policy supports this by identifying the risks and the steps we are taking to avoid them. It shows our commitment to developing a set of safe and responsible behaviours that will enable us to reduce the risks whilst continuing to benefit from the opportunities. Our expectations for responsible and appropriate conduct are formalised in our Acceptable Use Policies (AUP) which we expect all staff and pupils to follow.

As part of our commitment to E-Safety we also recognise our obligation to implement a range of security measures to protect the school network and facilities from attack, compromise and inappropriate use and to protect school data and other information assets. We have adopted the good practice requirements for all staff which are included in the Bradford Information Security Guidance on BSO (attached)

n.b. for the purposes of clarity and consistency throughout this document the person in school who is taking a lead on E-Safety is called the E-Safety coordinator**.**

The people in school taking on the role of E-Safety coordinator are Jonathan Nixon and Nicola Mason supported by other members of the SLT.

The following groups were consulted during the creation of this E-Safety policy: Staff, pupils and governors.

Policy Reviewed: January 2017

Next Review Date: January 2020

1. DCSF Guidance

Guidance for Safer Working Practices for Adults who work with Children and Young People DCSF Jan 2009

This guidance provides clear advice on appropriate and safe behaviors for all adults working with children in paid or unpaid capacities, in all settings and in all contexts. We acknowledge the guidance given in the following sections and accept this as part of our policy. (See extract in Appendix)

- Section 12 Communication with Children and Young People
- Section 27 Photography and Videos
- Section 28 Access to inappropriate images and Internet Usage

Responsibilities of the School Community

We believe that E-Safety is the responsibility of the whole school community and that everyone has their part to play in ensuring all members of the community are able to benefit from the opportunities that technology provides for learning and teaching. The following responsibilities demonstrate how each member of the community will contribute.

The Management Team accepts the following responsibilities:

- Identify a person (the E-Safety coordinator) (or team) to take responsibility for E-Safety and support them in their work.
- Ensure adequate technical support is in place to maintain a secure ICT system
- Ensure policies and procedures are in place to ensure the integrity of the school's information and data assets
- Ensure liaison with the Governors
- Develop and promote an E-Safety culture within the school community
- Ensure that all staff and pupils agree to the Acceptable Use Policy and that new staff have E-Safety included as part of their induction procedures
- Make appropriate resources, training and support available to all members of the school community to ensure they are able to carry out their roles effectively with regard to E-Safety
- Receive and regularly review E-Safety incident logs; ensure that the correct procedures are followed should an E-Safety incident occur in school and review incidents to see if further action is required
- Take ultimate responsibility for the E-Safety of the school community

Responsibilities of the E-Safety Coordinator

- Promote an awareness and commitment to E-Safety throughout the school
- Be the first point of contact in school on all E-Safety matters
- Lead the school E-Safety team
- Create and maintain E-Safety policies and procedures
- Develop an understanding of current E-Safety issues, guidance and appropriate legislation
- Ensure delivery of an appropriate level of training in E-Safety issues
- Ensure that E-Safety education is embedded across the curriculum
- Ensure that E-Safety is promoted to parents and carers
- Ensure that any person who is not a member of school staff , who makes use of the school ICT equipment in any context, is made aware of the Acceptable Use Policy

- Liaise with the Local Authority, the Local Safeguarding Children's Board and other relevant agencies as appropriate
- Monitor and report on E-Safety issues to the E-Safety group, the Leadership team and Governors as appropriate
- Ensure that staff and pupils know the procedure to follow should they encounter any material or communication that makes them feel uncomfortable
- Ensure an E-Safety incident log is kept up-to-date
- Ensure that Good Practice Guides for E-Safety are displayed in classrooms and around the school

Responsibilities of all Staff

- Read, understand and help promote the school's E-Safety policies and guidance
- Read, understand and adhere to the staff AUP
- Take responsibility for ensuring the safety of sensitive school data and information
- Develop and maintain an awareness of current E-Safety issues and legislation and guidance relevant to their work
- Maintain a professional level of conduct in their personal use of technology at all times
- Embed E-Safety messages in learning activities where appropriate
- Supervise pupils carefully when engaged in learning activities involving technology
- Ensure that pupils are told what to do should they encounter any material or receive a communication which makes them feel uncomfortable
- Report all E-Safety incidents which occur in the appropriate log and/or to their line manager
- Respect the feelings, rights, values and intellectual property of others in their use of technology in school and at home

Additional Responsibilities of Technical Staff

- Support the school in providing a safe technical infrastructure to support learning and teaching
- Ensure appropriate technical steps are in place to safeguard the security of the school ICT system, sensitive data and information. Review these regularly to ensure they are up to date
- At the request of the Leadership team conduct occasional checks on files, folders, email and other digital content to ensure that the Acceptable Use Policy is being followed
- Report any E-Safety-related issues that come to their attention to the E-Safety coordinator and/or leadership team
- Ensure that procedures are in place for new starters and leavers to be correctly added to and removed from all relevant electronic systems
- Ensure that suitable access arrangements are in place for any external users of the schools ICT equipment
- Liaise with the Local Authority and others on e-safety issues

Responsibilities of Pupils

- Read, understand and adhere to the pupil AUP and follow all safe practice guidance
- Take responsibility for their own and each others' safe and responsible use of technology wherever it is being used, including judging the risks posed by the personal technology owned and used by them outside of school
- Ensure they respect the feelings, rights, values and intellectual property of others in their use of technology in school and at home
- Understand what action should be taken if they feel worried, uncomfortable, vulnerable or at risk whilst using technology, or if they know of someone to whom this is happening
- Report all E-Safety incidents to appropriate members of staff
- Discuss E-Safety issues with family and friends in an open and honest way

Responsibilities of Parents and Carers

- Help and support the school in promoting E-Safety
- Read, understand and promote the pupil AUP with their children
- Discuss E-Safety concerns with their children, show an interest in how they are using technology, and encourage them to behave safely and responsibly when using technology
- Consult with the school if they have any concerns about their child's use of technology

Responsibilities of Governing Body

- Read, understand, contribute to and help promote the school's E-Safety policies and guidance as part of the schools overarching safeguarding procedures
- Support the work of the school in promoting and ensuring safe and responsible use of technology in and out of school, including encouraging parents to become engaged in E-Safety awareness
- Ensure appropriate funding and resources are available for the school to implement their E-Safety strategy

Responsibility of any external users of the school systems e.g. adult or community education groups; breakfast or afterschool club

- Take responsibility for liaising with the school on appropriate use of the school's ICT equipment and internet
- Ensure that participants follow agreed Acceptable Use Procedures

Acceptable Use Policies

School have a number of AUP for different groups of users.

These are shared with all users yearly and staff and pupils will be expected to agree to them and follow their guidelines. We will ensure that external groups and visitors to school who use our ICT facilities are made aware of the appropriate AUP.

School Acceptable Use Policy documents:

Pupils

Staff

Community Users

Learning and Teaching

We believe that the key to developing safe and responsible behaviours online for everyone within our school community lies in effective education. We know that the Internet and other technologies are embedded in our pupils' lives, not just in school but outside as well, and we believe we have a duty to help prepare our pupils to benefit safely from the opportunities that these present.

We will deliver a planned and progressive scheme of work to teach E-Safety knowledge and understanding and to ensure that pupils have a growing understanding of how to manage the risks involved in online activity.

We believe that learning about E-Safety should be embedded across the curriculum and also taught in specific lessons in ICT and PSCHE.

We will discuss, remind or raise relevant E-Safety messages with pupils routinely wherever suitable opportunities arise.

We will remind pupils about their responsibilities to which they have agreed through the AUP.

Staff and pupils will be reminded that third party content should always be appropriately attributed so as not to breach copyright laws.

How parents and carers will be involved

We believe it is important to help all our parents develop sufficient knowledge, skills and understanding to be able to help keep themselves and their children safe.

To achieve this we will offer opportunities for finding out more information through meetings, the school newsletter and website.

We request our parents to support the school in applying the E-Safety policy.

Managing and safeguarding ICT Systems

The school will ensure that access to the school ICT system is as safe and secure as reasonably possible.

Servers and other key hardware or infrastructure are located securely with only appropriate staff permitted access. Servers, workstations and other hardware and software are kept updated as appropriate. A firewall is maintained and virus and malware protection is installed on all appropriate hardware and is kept active and up-to-date. Staff have virus protection installed on all laptops used for school activity.

Any administrator or master passwords for school ICT systems are kept secure and available to at least two members of staff, e.g. head teacher and member of technical support.

The wireless network is protected by a secure log on which prevents unauthorized access. New users can only be given access by named individuals e.g. a member of technical support.

We do not allow anyone except technical staff to download and install software onto the network. Staff are allowed administrator rights to download software on school provided laptops.

Filtering Internet access

Web filtering of internet content is provided by Bradford Council and E-safe. This ensures that all reasonable precautions are taken to prevent access to inappropriate material. However it is not possible to guarantee that access to unsuitable material will never occur. Teachers are encouraged to check out websites they wish to use. All users are informed about the action they should take if inappropriate material is accessed or discovered on a computer. Notices are posted in classrooms and around school as a reminder.

Access

The school decides which users should and should not have Internet access, the appropriate level of access and the level of supervision they should receive. There are robust systems in place for managing network accounts and passwords, including safeguarding administrator passwords. Suitable arrangements are in place for visitors to the school who may be granted a temporary log in.

All users are provided with a log in appropriate to their key stage or role in school. Pupils are taught about safe practice in the use of their log in and passwords.

Staff are given appropriate guidance on managing access to laptops which are used both at home and school and in creating secure passwords.

Access to personal, private or sensitive information and data is restricted to authorised users only, with proper procedures being followed for authorising and protecting login and password information.

Remote access to school systems is covered by specific agreements and is never allowed to unauthorised third party users.

Using the Internet

We provide the internet to

- Support curriculum development in all subjects
- Support the professional work of staff as an essential professional tool
- Enhance the school's management information and business administration systems
- Enable electronic communication and the exchange of curriculum and administration data with the LA, the examination boards and others

Users are made aware that they must take responsibility for their use of, and their behaviour whilst using, the school ICT systems or a school provided laptop or device and that such activity can be monitored and checked.

All users of the school ICT or electronic equipment will abide by the relevant Acceptable Use Policy (AUP) at all times, whether working in a supervised activity or working independently,

Pupils and staff are informed about the actions to take if inappropriate material is discovered and this is supported by notices in classrooms and around school.

n.b. Additional guidance for staff is included in the School's Electronic Communications Guidance for Staff and this is included as part of the school's E-Safety Policy.

Using email

Email is regarded as an essential means of communication and the school provides all members of the school community with an e-mail account for school based communication. Communication by email between staff, pupils and parents will only be made using the school email account and should be professional and related to school matters only. E-mail messages on school business should be regarded as having been sent on headed notepaper and reflect a suitable tone and content and should ensure that the good name of the school is maintained. There are systems in place for storing relevant electronic communications which take place between school and parents.

Use of the school e-mail system is monitored and checked.

As part of the curriculum pupils are taught about safe and appropriate use of email. Pupils are informed that misuse of email will result in a loss of privileges.

Responsible use of personal web mail accounts by staff is permitted.

n.b. Additional guidance for staff is included in the School's Electronic Communications Guidance for Staff and this is included as part of the school's E-Safety Policy.

Publishing content online

e.g. using the School website, Learning Platform, blogs, wikis, podcasts, social network sites

School website:

The school maintains editorial responsibility for any school initiated web site or learning platform content to ensure that content is accurate and the quality of presentation is maintained. The school maintains the integrity of the school web site by ensuring that responsibility for uploading material is always moderated and that passwords are protected.

The point of contact on the web site is the school address, e-mail and telephone number. Published contact details for staff are school provided.

Identities of pupils are protected at all times. Photographs of identifiable individual pupils are not published on the web site and school obtains permission from parents for the use of pupils' photographs. Group photographs do not have a name list attached.

Creating online content as part of the curriculum:

As part of the curriculum we encourage pupils to create online content. Pupils are taught safe and responsible behaviour in their creation and publishing of online content. They are taught to publish for a wide range of audiences which might include governors, parents or younger children. Blogging, podcasting and other publishing of online content by pupils will take place within the school learning platform or other media selected by the school. Pupils will only be allowed to post or create content on sites where members of the public have access, when this is part of a school related activity. Appropriate procedures to protect the identity of pupils will be followed.

We take all steps to ensure that any material published online is the author's own work, gives credit to any other work included and does not break copyright.

Online material published outside the school:

Staff and pupils are encouraged to adopt similar safe and responsible behaviours in their personal use of blogs, wikis, social networking sites and other online publishing outside school as they are in school.

Material published by pupils, governors and staff in a social context which is considered to bring the school into disrepute or considered harmful to, or harassment of another pupil or member of the school community will be considered a breach of school discipline and treated accordingly.

n.b. Additional guidance for staff is included in the School's Electronic Communications Guidance for Staff and this is included as part of the school's E-Safety Policy.

Using images, video and sound

We recognise that many aspects of the curriculum can be enhanced by the use of multi-media and that there are now a wide and growing range of devices on which this can be accomplished. Pupils are taught safe and responsible behaviour when creating, using and storing digital images, video and sound.

Digital images, video and sound recordings are only taken with the permission of participants; images and video are of appropriate activities and are only taken of pupils wearing appropriate dress. Full names of participants are not used either within the resource itself, within the file-name or in accompanying text online.

We ask all parents/carers to sign an agreement about taking and publishing photographs and video of their children and this list is checked whenever an activity is being photographed or filmed.

For their own protection staff or other visitors to school never use a personal device (mobile phone, digital camera or digital video recorder) to take photographs of pupils.

n.b Additional guidance for staff is included in the School's Electronic Communications Guidance for Staff and this is included as part of the school's E-Safety Policy.

Using video conferencing and other online meetings

We use video conferencing to enhance the curriculum by providing learning and teaching activities that allow pupils to link up with people in other locations and see and hear each other. We ensure that staff and pupils take part in these opportunities in a safe and responsible manner. All video conferencing activity is supervised by a suitable member of staff. Pupils do not operate video conferencing equipment, answer calls or set up meetings without permission from the supervising member of staff.

Video conferencing equipment is switched off and secured when not in use and online meeting rooms are closed and logged off when not in use.

All participants are made aware if a video conference is to be recorded. Permission is sought if the material is to be published.

For their own protection a video conference or other online meeting between a member of staff and pupil(s) which takes place outside school or whilst the member of staff is alone is always conducted with the prior knowledge of the head teacher or line manager and respective parents and carers.

n.b. Additional guidance for staff is included in the School's Electronic Communications Guidance for Staff and this is included as part of the school's E-Safety Policy.

Using mobile phones

We recognise that the multimedia and communication facilities provided by a mobile phone can provide beneficial opportunities for pupils. However, their use in lesson time will only be with permission from the teacher.

School mobile phones or similar devices with communication facilities used for curriculum activities are set up appropriately for the activity. Pupils are taught to use them responsibly.

Where required for safety reason in off-site activities, a school mobile phone is provided for contact with pupils, parents or the school. Staff will not be expected to use personal mobile phones in any situation where their mobile phone number or other personal details may be revealed to a pupil or parent.

Unauthorised or secret use of a mobile phone or other electronic device, to record voice, pictures or video is forbidden. Unauthorised publishing of such material on a web site which causes distress to the person(s) concerned will be considered a breach of school discipline, whether intentional or unintentional. The person responsible for the material will be expected to remove this immediately upon request.

The sending or forwarding of text messages deliberately targeting a person with the intention of causing them distress, ‘cyberbullying’, will be considered a disciplinary matter.

n.b. Additional guidance for staff is included in the School’s Electronic Communications Guidance for Staff and this is included as part of the school’s E-Safety Policy.

Using other technologies

As a school we will keep abreast of new technologies and consider both the benefits for learning and teaching and also the risks from an E-Safety point of view.

We will regularly review the E-Safety policy to reflect any new technology that we use, or to reflect the use of new technology by pupils.

Staff or pupils using a technology not specifically mentioned in this policy will be expected to behave with similar standards of behavior to those outlined in this document.

Protecting school data and information

School recognises their obligation to safeguard staff and pupil's personal data including that which is stored and transmitted electronically. We regularly review our practices and procedures to ensure that they meet this basic obligation.

The school is a registered Data Controller under the Data Protection Act 1998 and we comply at all times with the requirements of that registration.

Pupils are taught about the need to protect their own personal data as part of their E-Safety awareness and the risks resulting from giving this away to third parties.

Staff are made fully aware of the contents of the Bradford's Information Security Guidance for Staff which is included as part of this policy.

Suitable procedures, and where necessary training, are in place to ensure the security of such data including the following:

- Staff are provided with encrypted USB memory sticks for carrying sensitive data
- All computers or laptops holding sensitive information are set up with strong passwords, password protected screen savers and screens are locked when they are left unattended
- Staff are provided with appropriate levels of access to the school's management information systems holding pupil data. Passwords are not shared and administrator passwords are kept securely
- Staff are aware of their obligation to keep sensitive data secure when working on computers outside school
- When we dispose of old computers and other equipment we take due regard for destroying information which may be held on them
- Remote access to computers is by authorised personnel only
- We have full back up and recovery procedures in place for school data
- Where sensitive staff or pupil data is shared with other people who have a right to see the information, for example Governors or the SIP, we label the material appropriately to remind them of their duty to keep it secure and securely destroy any spare copies

Dealing with E-Safety incidents

All E-Safety incidents are recorded in the School E-Safety Log which is regularly reviewed.

Any incidents where pupils do not follow the Acceptable Use Policy will be dealt with following the school's normal behaviour or disciplinary procedures.

In situations where a member of staff is made aware of a serious E-Safety incident, concerning pupils or staff, they will inform the E-Safety coordinator, their line manager or head teacher who will then respond in the most appropriate manner.

Instances of cyberbullying will be taken very seriously by the school and dealt with using the schools anti-bullying procedures. School recognises that staff as well as pupils may be victims and will take appropriate action in either situation.

Incidents which create a risk to the security of the school network, or create an information security risk, will be referred to the school's E-Safety coordinator and technical support and appropriate advice sought and action taken to minimize the risk and prevent further instances occurring, including reviewing any policies, procedures or guidance. If the action breaches school policy, then appropriate sanctions will be applied. The school will decide if parents need to be informed if there is a risk that pupil data has been lost.

School reserve the right to monitor equipment of their premises and to search any technology equipment, including personal equipment with permission, when a breach of this policy is suspected.

Dealing with a Child Protection issue arising from the use of technology:

If an incident occurs which raises concerns about Child Protection or the discovery of indecent images on the computer, then the procedures outlined in the Bradford Safeguarding Board Procedures and Guidance will be followed.

Dealing with complaints and breaches of conduct by pupils:

- Any complaints or breaches of conduct will be dealt with promptly
- Responsibility for handling serious incidents will be given to a senior member of staff
- Parents and the pupil will work in partnership with staff to resolve any issues arising
- There may be occasions when the police must be contacted. Early contact will be made to establish the legal position and discuss strategies*.*

The following activities constitutes behavior which we would always consider unacceptable (and possible illegal):

- accessing inappropriate or illegal content deliberately
- deliberately accessing downloading and disseminating any material deemed offensive, obscene, defamatory, racist, homophobic or violent
- continuing to send or post material regarded as harassment, or of a bullying nature after being warned

- using digital communications to communicate with pupils in an inappropriate manner (for instance, using personal email accounts, personal mobile phones, or inappropriate communication via social networking sites)

The following activities are likely to result in disciplinary action:

- any online activity by a member of the school community which is likely to adversely impact on the reputation of the school
- accessing inappropriate or illegal content accidentally and failing to report this
- inappropriate use of personal technologies (e.g. mobile phones) at school or in lessons
- sharing files which are not legitimately obtained e.g. music files from a file sharing site
- using school or personal equipment to send a message, or create content, that is offensive or bullying in nature or could bring the school into disrepute
- attempting to circumvent school filtering, monitoring or other security systems
- circulation of commercial, advertising or 'chain' emails or messages
- revealing the personal information (including digital images, videos and text) of others by electronic means (e.g. sending of messages, creating online content) without permission
- using online content in such a way as to infringe copyright or which fails to acknowledge ownership (including plagiarising of online content)
- transferring sensitive data insecurely or infringing the conditions of the Data Protection Act, revised 1988

The following activities would normally be unacceptable; however in some circumstances they may be allowed e.g. as part of planned curriculum activity or as system administrator to problem solve

- accessing social networking sites, chat sites, instant messaging accounts, email or using a mobile phone for personal use during lesson time
- accessing non-educational websites (e.g. gaming or shopping websites) during lesson time
- sharing a username and password with others or allowing another persona to log in using your account
- accessing school ICT systems with someone else's username and password
- deliberately opening, altering, deleting or otherwise accessing files or data belonging to someone else

References to related documents:

- Acceptable Use Policies (Pupils, Staff, Visitors and Supply staff, Community users)
- Letter for Parents explaining the AUP and agreement to sign
- School's Electronic Communications Guidance for Staff
- Bradford Information Security Guidance for Staff
- Practical Guidance for protecting school information

Appendix 1

Extract from:

Guidance for Safer Working Practice for Adults who work with Children and Young People. DCSF January 2009

Section 12 Communication with Children and Young People *(including the Use of Technology)*

Communication between children and adults, by whatever method, should take place within clear and explicit professional boundaries. This includes the wider use of technology such as mobile phones text messaging, e-mails, digital cameras, videos, web-cams, websites and blogs. Adults should not share any personal information with a child or young person. They should not request, or respond to, any personal information from the child/young person, other than that which might be appropriate as part of their professional role. Adults should ensure that all communications are transparent and open to scrutiny.

Adults should also be circumspect in their communications with children so as to avoid any possible misinterpretation of their motives or any behaviour which could be construed as grooming. They should not give their personal contact details to children and young people including e-mail, home or mobile telephone numbers, unless the need to do so is agreed with senior management and parents/carers. E-mail or text communications between an adult and a child young person outside agreed protocols may lead to disciplinary and/or criminal investigations. This also includes communications through internet based web sites.

Internal e-mail systems should only be used in accordance with the organisation's policy.

This means that the organisation should:

- *have a communication policy which specifies acceptable and permissible modes of communication*

This means that adults should:

- *not give their personal contact details to children or young people, including their mobile telephone number and details of any blogs or personal websites*
- *only use equipment e.g. mobile phones, provided by organisation to communicate with children, making sure that parents have given permission for this form of communication to be used*
- *only make contact with children for professional reasons and in accordance with any organisation policy*
- *recognise that text messaging is rarely an appropriate response to a child in a crisis situation or at risk of harm. It should only be used as a last resort when other forms of communication are not possible*
- *not use internet or web-based communication channels to send personal messages to a child/young person*
- *ensure that if a social networking site is used, details are not shared with children and young people and privacy settings are set at maximum*

Section 27 Photography and Videos

Working with children and young people may involve the taking or recording of images. Any such work should take place with due regard to the law and the need to safeguard the privacy, dignity, safety and well being of children and young people. Informed written consent from parents or carers and agreement, where possible, from the child or young person, should always be sought before an image is taken for any purpose.

Careful consideration should be given as to how activities involving the taking of images are organised and undertaken. Care should be taken to ensure that all parties understand the implications of the image being taken especially if it is to be used for any publicity purposes or published in the media, or on the Internet. There also needs to be an agreement as to whether the images will be destroyed or retained for further use, where these will be stored and who will have access to them.

Adults need to remain sensitive to any children who appear uncomfortable, for whatever reason, and should recognise the potential for such activities to raise concerns or lead to misunderstandings.

It is not appropriate for adults to take photographs of children for their personal use.

This means that adults should:

- be clear about the purpose of the activity and about what will happen to the images when the activity is concluded
- be able to justify images of children in their possession
- avoid making images in one to one situations or which show a single child with no surrounding context
- ensure the child/young person understands why the images are being taken and has agreed to the activity and that they are appropriately dressed.
- only use equipment provided or authorised by the organisation
- report any concerns about any inappropriate or intrusive photographs found
- always ensure they have parental permission to take and/or display photographs

This means that adults should not:

- display or distribute images of children unless they have consent to do so from parents/carers
- use images which may cause distress
- use mobile telephones to take images of children
- take images ‘in secret’, or taking images in situations that may be construed as being secretive.

Section 28 Access to Inappropriate Images and Internet Usage

There are no circumstances that will justify adults possessing indecent images of children. Adults who access and possess links to such websites will be viewed as a significant and potential threat to children. Accessing, making and storing indecent images of children on the internet is illegal. This will lead to criminal investigation and the individual being barred from working with children and young people, if proven.

Adults should not use equipment belonging to their organisation to access adult pornography; neither should personal equipment containing these images or links to them be brought into the

workplace. This will raise serious concerns about the suitability of the adult to continue to work with children.

Adults should ensure that children and young people are not exposed to any inappropriate images or web links. Organisations and adults need to ensure that internet equipment used by children have the appropriate controls with regards to access. e.g. personal passwords should be kept confidential.

Where indecent images of children or other unsuitable material are found, the police and Local Authority Designated Officer (LADO) should be immediately informed. Adults should not attempt to investigate the matter or evaluate the material themselves, as this may lead to evidence being contaminated which in itself can lead to a criminal prosecution.

This means that organisations should

- have clear e-safety policies in place about access to and use of the internet
- make guidance available to both adults and children and young people about appropriate usage.

This means that adults should:

- follow their organisation's guidance on the use of IT equipment
- ensure that children are not exposed to unsuitable material on the internet
- ensure that any films or material shown to children and young people are age appropriate

Information Security, Data Protection and Freedom of Information
Guidance from Bradford Schools online

Schools are already doing good work to safeguard learners while they are using ICT but this good practice and awareness is not always reflected in the way schools handle personal and sensitive information.

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

The following guidance is based on information provided by the Information Commissioner's Office (ICO) and CESG (Communications-Electronics Security Group, the Government's national technical authority for information assurance).

What is the risk?
The risk associated with the loss of data depends on the data. The biggest risk is that the data may be accessed by someone who should not have access to it. Such inappropriate access may lead to embarrassment for the individual(s) whose data is lost, embarrassment for the school and, in the worst case, child protection issues.

It is a legal requirement of the Data Protection Act 1998 to protect and secure personal data. The Information Commissioner's Office (ICO) recommends that portable and mobile devices (including media [eg USB sticks, CDs]) used to store and transmit personal information, the loss of which could cause damage or distress to individuals, should be protected using approved encryption software which is designed to guard against the compromise of information.

What data do I need to protect?
You should secure any personal data you hold about individuals and any data that is deemed sensitive or valuable to your organisation.

It is good practice to protectively mark personal data. This will help people handling it understand the need to keep it secure and to destroy it when it is no longer needed. This is especially important if personal data information is combined into a report and printed.

What is Encryption?
Encryption is the process of scrambling data so it can't be read without supplying the appropriate electronic key or password to unscramble, or decrypt, the data.

The Information Commissioner's Office (ICO) recommends that portable and mobile devices (including media) used to store and transmit personal information should be protected using encryption software.

Personal or sensitive data that is removed or accessed from outside an approved secure space should be encrypted. Examples of approved secure spaces include physically secure areas in schools, colleges, universities, local authorities and the premises of support contractors.

Although recommended for protecting data in the UK, some countries ban the use, or severely regulate the import, export or use of, encryption technology. You should always check current restrictions before leaving the UK with encryption software or encrypted data.

What is personal data?

According to the Data Protection Act 1998:

"'Personal data' means data which relate to a living individual who can be identified –

1. From those data, or
2. From those data and other information which is in the possession of, or is likely to come into the possession of, the data controller,

And includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual."

In a school context this will include pupil and staff names, addresses, UPNs, SEN statements and any data in your Management Information System (eg SIMS).

How do I use encryption to protect my laptop and USB memory stick?

Laptops, by their nature, are easily stolen or lost. It is easy for a thief or someone who finds your lost laptop to bypass the Windows password and access all the files on it unless it is encrypted. The same is true for your USB memory stick.

If you are carrying personal data on your laptop or USB stick then you have a legal obligation to protect that data. The easiest way to protect these systems is using encryption software.

Laptops can be encrypted using full disk encryption or file based encryption. The easiest solution is full disk encryption. This scrambles the entire contents of your laptops hard disk and any files you create or copy to it. With full disk encryption you normally need to enter a password to decrypt (unscramble) the disk when you turn on the laptop, followed by your normal Windows password. Once you have logged in you will not notice any difference to the way the laptop operates. Any files that you copy to, or create on, your laptop will be automatically encrypted. Files stay encrypted while ever they are on the laptop hard disk. If you copy a file to an unencrypted USB memory stick the copy of the file on the memory stick will not be encrypted.

There are two options for encrypting files on a USB memory stick. You can encrypt individual files or folders (file based encryption) or use a solution that encrypts the entire contents of the USB memory stick. Which you use may depend on how many files you are storing, how often you use the memory stick and cost. The easiest, but most expensive option is to use a hardware encrypted USB stick. A cheaper alternative would be to use software encryption to scramble the whole USB memory stick, but this is more difficult to set up. Tools such as Winzip or 7Zip can be used to encrypt individual files.

Is there a safe way to send data by email?

Email is not a secure way to transfer files. You do not know the route your email will take to get to the recipient (it may go all the way round the world to reach someone in the next street). Any email server your message passes through may store a copy of your message and any attachments. It is advisable to use alternative secure mechanisms to transfer files.

If there are no suitable alternatives to using email then any personal or sensitive data is best sent as an encrypted attachment. This may mean writing your email as a Word document, encrypting the Word document and sending this as an email attachment. Word files can be encrypted using tools such as WinZip or 7Zip. If sending encrypted attachments always use an alternative communication method, such as a text or phone call, to send the password for the encrypted file. This way, if the email is intercepted, the person who intercepts the email does not have access

to the password. This also protects your email should you accidentally send the email to the wrong person.

What else do I need to consider?

Social engineering and Phishing: Wikipedia describes social engineering and phishing as follows:

Social engineering is commonly understood to mean the art of manipulating people into performing actions or divulging confidential information. While it is similar to a confidence trick or simple fraud, the term typically applies to trickery or deception for the purpose of information gathering, fraud, or computer system access; in most cases the attacker never comes face-to-face with the victims.

Phishing is a way of attempting to acquire information such as usernames, passwords, and credit card details by masquerading as a trustworthy entity in an electronic communication. Communications purporting to be from popular social web sites, auction sites, online payment processors or IT administrators are commonly used to lure the unsuspecting public. Phishing is typically carried out by e-mail spoofing or instant messaging, and it often directs users to enter details at a fake website whose look and feel are almost identical to the legitimate one.

Hoaxes, scams and chain letters: Hoaxes and scams do not normally carry viruses or ask you for personal information; instead they are designed to cause confusion, worry and inconvenience. They are often passed on by well-intentioned friends and colleagues. It is good practice to verify the content of an email before forwarding it on. A good place to do this is http://www.hoax-slayer.com/

Physical security: You will already have secure reception areas in your school but do you have a robust process for cancelling lost swipe cards and passes? If you invite contractors or parents into staff only areas of your premises such as the staff room, what information can they see displayed on whiteboards, noticeboards or left on printers. Sensitive paperwork should be kept in locked filing cabinets and shredded when it is no longer required.

Conversations: Be aware of who is around when you have a conversation. If you are on the telephone you should consider closing your office door, or moving to a more private place with your mobile phone if you are discussing anything of a sensitive nature.

IT disposal: It is good practice to securely wipe the hard disks of PCs and Laptops before they are sent for disposal or recycling. Deleting files, and even formatting the hard disk does not remove the file from the hard disk, it just hides it from Windows and makes the disk space available to written to. Securely deleting the hard disk ensures that any sensitive files that may have been written any time during the lifetime of that computer are destroyed.

What standards should I look for when buying security products?

Anti-Virus

Antivirus solutions should be certified by ICSA (www.icsalabs.com).

Encryption

A number of encryption solutions are available, some of which may be certified as CAPS (CESG Assisted Products Service), CCTM (CESG Claims Tested Mark) approved, FIPS (Federal Information Processing Standards) 140-2 compliant or have no formal certification.

Certified products have been independently evaluated to verify that they operate correctly and are robust. Ideally, organisations should use certified products where possible. The certification process, however, is expensive and time-consuming, so certified solutions tend to be more

expensive and respond more slowly to changes to operating systems or applications. Non-certified solutions can also provide effective data security.

Paper Shredders

Should conform to DIN 32 757 level 3 or higher. This means the shreds are at most 4mm wide and 80mm long. Most cross cut shredders are DIN 32 757 level 3 or higher.

Where can I find further information?

Advice on the Data Protection Act, the Freedom of Information Act and all related issues is provided by BMDC. Please contact Tracey Parry in Children's Services on 01274 385901, or the BMDC legal team on 01274 432233

Get Safe Online is "a joint initiative between the Government, law enforcement, leading businesses and the public sector. Our aim is to provide computer users and small businesses with free, independent, user-friendly advice that will allow them to use the internet confidently, safely and securely." Their website can be found at http://www.getsafeonline.org/

The Information Commissioners Office (ICO) is the UK's independent public body set up to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals. Their website can be found here: http://www.ico.gov.uk/

CESG protects the vital interests of the UK by providing policy and assistance on the security of communications and electronic data, working in partnership with industry and academia.

CESG are the UK Government's National Technical Authority for Information Assurance (IA). http://www.cesg.gov.uk

CEOP (Child Exploitation and Online Protection Command) works with child protection partners across the UK and overseas to identify the main threats to children and coordinates activity against these threats to bring offenders to account. They protect children from harm online and offline, directly through NCA led operations and in partnership with local and international agencies. https://www.ceop.police.uk/safety-centre

Think U Know The CEOP Command's Thinkuknow programme provides resources, training and support for professionals who work directly with children and young people. https://www.thinkuknow.co.uk