Brownhill Primary School

E-Safety Policy

Feb 2017

CEOP ADVICE
ceop.police.uk

Introduction

The school makes widespread use of modern technology in the belief and understanding that it can develop and enhance all aspects of teaching and learning, as well as providing a preparation for life in a society where the use of ICT is widespread.

The statutory curriculum expects pupils to learn how to locate, retrieve and exchange information using ICT.

This policy

- **applies to all users of ICT equipment, in its widest sense, whilst on school premises. It also applies to anyone who uses school ICT equipment, software or electronic data whilst off the premises.**
- **forms part of the school's ICT subject policy and ICT acceptable use policy.**
- **relates to other school policies including, child protection, behaviour and bullying.**
- **also relates to the Leeds Learning Network Internet Access Policy & Email Code of Practice.**
- **often refers to the internet due to this being the major concern. However, it should be noted that there are other aspects of e-safety that need consideration.**

It is difficult to consider every eventuality within this policy due to the nature of rapid technological change within short timescales.

E-Safety

The increased use of technology at work and at home exposes people to a number of risks and dangers. In its simplest form e-safety is about ensuring people use electronic technologies in a way which will keep them safe without limiting their opportunities for creation and innovation.

The Internet is fantastic for information and great for communication, but we all need to know how to use it safely. The children are likely to have internet access in more than one place, so it is important to equip them with the skills to handle this technology safely.

E-safety is also about protecting the hardware and software we use from attack by unscrupulous people, who may wish to cause disruption or commit illegal acts.

E-safety is also about protecting electronic data, our private, personal data and that of other people.

Responsibilities

The use of computer systems without permission or for purposes not agreed by the school could constitute a criminal offence under the Computer Misuse Act 1990.

Everyone who uses ICT connected with the school has a responsibility to have a regard for e-safety.

The Government has placed a responsibility on the Governors and Management of the school to ensure that all employees and pupils are aware of e-safety concerns and procedures, and that they receive training to raise their awareness of the issues involved.

The teaching staff have a responsibility, as part of the statutory requirements of the curriculum, to teach e-safety.

Although the ultimate responsibility lies with the Governing Body and the Headteacher, the school will nominate

- **an E-Safety Coordinator – Jacqui Emmett**
- **a Governor with responsibility for e-safety issues (tba)**
- **a member of the senior management team to deal with e-safety issues and e-safety complaints in particular – Sue Holliday**

The E-Safety Coordinator will

- **oversee the development of this policy**
- **oversee the implementation of this policy**
- **advise the school management on e-safety issues**
- **advise staff on e-safety teaching and learning resources**
- **be a point of contact for anyone connected with the school who has questions or concerns about e-safety issues**
- **be available to deal with general issues of e-safety that are not specific complaints concerning individuals (for example: informing LLN of an inappropriate website or a security issue)**
- **be available to deal with minor infringements of the e-safety policy and rules, including accidental infringements**
- **pass on to a nominated senior manager or Headteacher any complaint or evidence received concerning individual pupils or staff misuse of ICT**

The Headteacher is the school's official administrator for the Leeds Learning Network. However, they may delegate part of this responsibility to other members of staff.

Staff who manage the filtering systems or monitor ICT use will be supervised by a member of the senior management team and work to clear procedures for reporting issues, testing filtering restrictions and checking security systems.

Teaching and learning

Why the Internet and Digital Communications are Important

The Internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide pupils with quality Internet access as part of their learning experience.

Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils.

Internet Use Will Enhance Children's Learning

The school Internet access will be specifically tailored for pupil use and will include filtering appropriate to the age of pupils.

Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.

Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation

Pupils will be shown how to publish and present information to a wider audience.

Pupils Will be Taught How to Evaluate Internet Content

The school aims to ensure that the use of Internet derived materials by pupils complies with copyright law.

Pupils will be taught the importance of cross-checking information before accepting its accuracy.

Pupils will be taught how to report unpleasant Internet content e.g. to an adult, or using the CEOP Report Abuse icon

Equal Opportunities

The school believes that it is essential that opportunities are provided for everyone to access ICT, regardless of gender, race, religion, culture, ethnic group, physical ability or mental ability.

Special Needs

ICT can be a positive tool for children with Special Educational Needs. Access to the Internet is therefore a vital link with which communication to the outside world can be achieved. Access to the Internet can also stimulate children to develop their ideas and research independently.

The school will endeavour to ensure that children with Special Educational Needs are made aware of the risks and dangers of using ICT, within their understanding and abilities. The ICT Coordinator will make appropriate resources available to facilitate this.

Managing School Network Access

The school will maintain two network systems under the control of two separate file servers

- **admin (school administration network)**
- **curriculum**

The Headteacher will nominate a senior member of staff to oversee the use of the admin network.

The ICT Coordinator/ICT Technician will have responsibility for the administration of the curriculum network.

Both servers / networks will be protected by Sophos antivirus software, provided through Education Leeds, which will be updated on a daily basis.

School ICT systems security will be regularly reviewed.

Security strategies will be implemented according to guidance from Education Leeds.

Full access to the admin network will be restricted to Headtacher, ICT Technician and office staff. Other employees may be allowed limited access to this network for specific tasks, at the discretion of the Headteacher.

Levels of access to the admin network will be enforced through unique usernames and passwords.

The admin network will be the only network to contain the full details of all employees and pupils. SIMs etc.

All staff and pupils of the school will be allowed access to the curriculum network.

Staff will have their own username and unique password in order to use the curriculum network. They will be allocated their own file space and have access to a shared “staff only” area of the network, which the pupils will not be able to access. Staff will also be able to access all pupil folders.

Pupil access will be arranged at different levels appropriate to the age of the children, through a structured menu system.

All pupils from Y1 to Y6 will be allocated their own username and file space. They will also have access to a “shared area” containing general resources.

Foundation stage children will use a group username and password. Most of the time adults will log-on for them.

Children will not be allowed access to computer equipment at playtimes and lunchtimes unless a member of staff is present in the room.

Children will not be allowed to work in the ICT Suite without staff supervision. Children working in library computer areas during lesson times will not be allowed access to the Internet without adult supervision.

Parents, visitors, guests and supply staff may be granted restricted access to the curriculum network, with permission from the Headteacher or ICT Coordinator, through the use of special usernames and passwords.

Contracted I.T. technicians may be given full access to either network, at the discretion of the Headteacher.

Only the ICT Coordinator, computer technicians, or other persons nominated by the Headteacher, may install software on any school workstation or server.

Managing Internet Access

The Internet Service Provider for the school will be the Leeds Learning Network (LLN).

Statutory UK ISP monitoring laws insist that LLN record all Internet usage and E-mail.

The Leeds Learning Network will inform the Headteacher if they suspect any misuse of LLN.

The Headteacher will be the nominated administrator for the school's LLN services.

The Headteacher has access to a special LLN account that allows the administrator to use the LLN with all the restrictions and filters turned off.

According to LLN regulations, the Headteacher and Chair of the Governing Body are ultimately responsible for the proper allocation and use of this account.

The Headteacher must be the only person who uses this account.

A written record must be kept of any use of this account.

Any school website or "learning platform" will be hosted through the LLN.

All staff will have their own LLN user account with a unique username and password.

Staff must adhere to the school's "Internet Access Policy" (Appendix 1) when accessing the internet.

Staff are not allowed to access the internet other than through the LLN whilst on the school premises.

All key stage 2 pupils, Y3 to Y6, will have their own LLN user account with a unique username and password.

There must be a member of staff present in the room when key stage 2 pupils are accessing the Internet or using e-mail.

Foundation and key stage 1 pupils' access to the Internet will be by adult demonstration with directly supervised access to specific, approved, on-line materials. They will not have their own LLN username but will use special class group accounts (called "Rainbow" accounts).

Foundation and key stage 1 pupils must be closely supervised by an adult when accessing materials using the Internet.

Pupils must adhere to the school's "Rules for Responsible Pupil Internet Use" (Appendix 2) when accessing the internet.

Pupils are not allowed to access the internet other than through the LLN whilst on the school premises.

Managing Access to E-mail

Incoming e-mail should be treated as suspicious and attachments not opened unless the author is known.

Teachers should consider how e-mail from pupils to external bodies is to be presented and controlled before allowing it.

The forwarding of chain letters or anonymous mail is not permitted.

In-coming and outgoing email will be regarded as public and will be monitored by LLN.

Staff will have access to e-mail through their LLN account.

Staff LLN e-mail accounts are for school related use and can only be used for private purposes at the discretion of the Headteacher. No private business activities of any nature may be undertaken.

Staff may only access a private or home e-mail account on school premises outside normal timetabled hours. However, this should be kept to a minimum and staff should follow the school's "Internet Access Policy" (Appendix 1) when doing so. The Headteacher reserves the right to withdraw this arrangement at any time.

Staff should inform the Headteacher if they receive offensive e-mail.

Key stage 2 pupils, Y3 to Y6, will have access to e-mail through their LLN account. Pupils must adhere to the "Rules for Responsible Pupil Internet Use" (Appendix 2) when using e-mail.

Pupils are not allowed to access a private or home e-mail account on school premises.

Pupils must immediately tell a teacher if they receive offensive e-mail.

Foundation and key stage 1 pupils will not be allowed access to e-mail on school premises, unless under supervision.

Managing Other Technologies

Published Content and the School Website or Learning Platform

Staff or pupil personal contact information will not generally be published. The contact details given online should be the school office or Headteacher.

The Headteacher will take overall editorial responsibility and ensure that content is accurate and appropriate.

All material published on the school website must be the author's own work. If material from other sources is included credit should be given to the original author, stating clearly the source of such work and must not break copyright laws.

Work belonging to a pupil can only be published with the permission of the pupil and their parents / carers.

Photographs that include pupils will be selected carefully so that individual pupils cannot be identified or their image misused. Consideration should be given to using a group photograph rather than full-face photos of individual children.

Pupils 'full' names will not be used anywhere on the school website or learning platform, particularly in association with photographs.

Pupil image file names will not refer to the pupil by name.

Parents should be clearly informed of the school policy on image taking and publishing, both on school and independent electronic repositories

Social Networking and Personal Publishing

Pupils will not be allowed to access social networking sites, instant messaging sites or chat rooms, on school premises.

Pupils will not be allowed access to YouTube or similar websites on school premises.

Newsgroups may not be used by pupils unless specifically approved by their teacher.

Pupils will be advised never to give out personal details of any kind which may identify them, their friends or their location.

Pupils and parents will be advised that the use of social network spaces outside school brings a range of dangers for primary aged pupils. Ideally pupils should use only moderated, child friendly, social networking sites. Pupils will be advised to use nicknames and avatars when using such social networking sites.

It is not advisable for staff to allow pupils to name them in any "friends" or contacts list on a social networking site, unless they are actually a relation of the pupil.

It is not advisable for staff to add pupils to their own "friends" or contacts list on a social networking site, unless they are actually a relation of the pupil.

Managing Videoconferencing and Webcam Use

Videoconferencing should use the educational broadband network to ensure quality of service and security.

Pupils must ask permission from the supervising teacher before making or answering a videoconference call.

Videoconferencing and webcam use must be appropriately supervised for the pupils' age.

Mobile Phones

All staff should note that technologies such as mobile phones with wireless Internet access can bypass school filtering systems and present a new route to undesirable material and communications.

Pupils are not allowed to use mobile phones, or technologies built in to a mobile phone, on school premises or during school activities off-site.

Staff should not use their own mobile phone to capture photographs of pupils.

Digital Cameras

It should be noted that there are risks to allowing the capturing digital images on the school premises. It is easy for anyone to manipulate digital images, using modern software, and put them to inappropriate uses.
For example:

> **Pupils using images to bully other pupils or staff;**
> **Pupils manipulating an image and publishing a compromising version on the internet.**

It should be noted that digital cameras can be used to spread computer viruses, in a similar way to memory sticks.

Staff and pupils may use digital cameras belonging to the school, as part of the curriculum, to provide evidence or as a record of work.

Staff should not capture images of pupils on personal digital cameras.
Staff who do so would put themselves at risk should a pupil or parent brings a complaint against them. It would be harder to prove that the images were taken for school purposes, especially if the images were taken home on the camera.

Digital copies of images of staff or pupils must not be e-mailed or given to someone outside the school premises without permission from the Headteacher.

Images taken with a school digital camera should be kept in the cameras memory, or on the memory card, for as short a time as possible and then be deleted. Images should not be stored on a camera for long periods and certainly not indefinitely.

Pupils should not be allowed to use personal digital cameras on the school premises unless permission is granted by the Headteacher for a specific use, and only then under close supervision and with great care.

If sanctioned by the Headteacher, pupils will be allowed to use personal digital cameras on a school activity off the premises. Close supervision would be essential and limits should be explained to the pupils.

Staff should note that some games machines including the Sony Playstation, Microsoft Xbox, Nintendo DSi and other hand-held consoles, have a built in webcam. It is not advisable to allow their use in school. Staff should get permission from the Headteacher before allowing the use of such devices in school.

Laptops

When on the school premises, pupils may only use laptops provided by the school. They are not allowed to bring personal laptops on to school premises.

Staff provided with a laptop purchased by the school can only use it for private purposes at the discretion of the Headteacher. Such laptops remain the property of the school and are open to scrutiny by senior management, contracted technicians and the ICT Coordinator.

Laptops belonging to the school must have active antivirus software installed and be password protected.

Staff provided with a laptop purchased by the school, are responsible for regularly updating the antivirus software.

Staff intending to bring personal / private laptops on to the school premises should consider very carefully if it is appropriate. There are security risks and also risks associated with any private content on the laptop.

Staff must not attach a personal / private laptop to an interactive whiteboard when children are present.

The security of school laptops is of prime importance due to their portable nature and their being liable to theft.

WiFi

There may be devices on the premises that use WiFi or other wireless connection. It is extremely important that such connections have the maximum possible security levels activated.

Staff should note that WiFi connections can be intercepted by unauthorized persons, depending on the range of the transmission and what security systems are activated.

Interactive Whiteboards (IWB)

Staff must be careful when using an IWB with pupils when they are logged on using their personal username and password. This may give pupils access to files and areas of the network that are restricted to staff use only.

Staff must not deliberately log-on to an IWB system using their personal username and password in order to circumvent the normal security and filtering systems, allowing pupils access to things that they would not normally be allowed to use.

Emerging Technologies

Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.

Technologies not specifically covered by this policy can only be used on school premises at the discretion of the Headteacher.

It should be noted that Games machines including the Sony Playstation, Microsoft Xbox, Nintendo DSi and other hand-held consoles, have Internet access which may not include any filtering. Care is required if permission is granted for use in school or other officially sanctioned location. Such devices may also be capable of instant messaging when in close proximity to others, without using the internet. It is not advisable to allow their use in school. Staff should get permission from the Headteacher before allowing the use of such devices in school.

Authorising Access

The final decision as to who can be granted access to school ICT equipment and facilities will rest with the Headteacher.

The ICT Coordinator / ICT Technician will be responsible for supervising access to the curriculum network and classroom ICT equipment.

The Headteacher is responsible for supervising access permissions to the LLN but may delegate some of this responsibility to other members of staff.

The school will maintain a current record of all staff and pupils who are granted access to school ICT systems.

Protecting Personal Data

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.

Every member of staff must take all reasonable steps to securely protect all data concerning pupils and others.

All school computer systems must be password and virus protected, including school equipment used at home by staff.

Any data taken off the school premises should be kept to a minimum and if no longer required, deleted or destroyed in an appropriate manner, or returned to school for destruction.

All printed copies of personal data must be shredded before disposal as waste material.

Staff must take all reasonable care when using, storing and transporting memory sticks, CDs or DVDs containing school data.

Memory sticks provided by school must not be used for private purposes and remain open to scrutiny by senior management, contracted technicians and the ICT Coordinator.

Anyone transferring personal data from school sources to their own personal computer or memory stick is personally liable for the security of the data and for any legal consequences.

When working with personal or confidential data computer screens should be positioned where they are not easily visible from outside the immediate work area or by an unauthorized person.

Assessing Risks

The school will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a computer connected to the school network. The school, Education Leeds, the Leeds Learning Network and Leeds City Council do not accept liability for any material accessed, or any consequences of ICT or Internet access, either on school premises or through the Leeds Learning Network.

Handling E-Safety Complaints

Complaints of ICT / Internet misuse will be dealt with by the ICT Co-ordinator / ICT technician, who will deal with the issue appropriately.

Any complaint about staff misuse must be referred to the Headteacher, who will decide if any sanctions are to be imposed.

Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.

The Headteacher will arrange contact / discussions with Education Leeds and the Police Authority to establish clear procedures for handling potentially illegal issues.

Any complaint about illegal misuse must be referred to the Headteacher, who will decide if a referral to the police or other relevant authority is necessary, following any guidelines issued by Education Leeds.

Staff should note that copies of illegal material they find should not be sent / forwarded to anyone else, even as evidence, as this could also be seen an committing an illegal act.

Do not e-mail copies of illegal material to the Headteacher, E-Safety Coordinator, Child Protection Coordinator or the LLN Service Desk, as receiving such material could also be seen as the committing of an illegal act on their part.

Communicating Policy

Introducing the E-Safety Policy to Pupils

E-Safety rules will be posted in all rooms where computers are used and discussed with pupils regularly.

Pupils will be informed that network and Internet use will be monitored and appropriately followed up.

A programme of training in e-Safety will be developed, possibly based on the materials from CEOP.

E-Safety training will be embedded within the ICT scheme of work and the Personal Social and Health Education (PSHE) curriculum.

Staff and the E-Safety Policy

All staff will be given the School E-Safety Policy and its importance explained.

Appropriate training will be arranged for all staff.

All temporary staff and supply staff used regularly by the school will be given the School E-Safety Policy and its importance explained.

Every member of staff, whether permanent, temporary or supply staff regularly used by the school, must be informed that network and Internet traffic will be monitored and can be traced to the individual user.

Enlisting Parents' and Carers' Support

E-Safety policy will be published on School Website.

Links to useful internet websites, with advice for parents, will be built in to the school website

Visitors and the E-Safety Policy

Not all visitors will need to use school ICT but those who do will need to be informed that the school does have an E-Safety policy and they should be given the opportunity to read it, if the Headteacher thinks that it would be appropriate.

Visitors using school ICT must be informed that network and Internet traffic will be monitored and can be traced to the individual user.