

CONTENTS

Contents

INTRODUCTION	1
MONITORING	3
BREACHES	4
Incident Reporting	4
ACCEPTABLE USE AGREEMENT: PUPILS	5
ACCEPTABLE USE AGREEMENT: STAFF, GOVERNORS AND VISITORS	7
COMPUTER VIRUSES	8
E-MAIL	9
Managing e-Mail	9
Sending e-Mails	10
Receiving e-Mails	10
e-mailing Personal, Sensitive, Confidential or Classified Information	10
EQUAL OPPORTUNITIES	12
Pupils with Additional Needs	12
ESAFETY	13
eSafety - Roles and Responsibilities	13
eSafety in the Curriculum	13
eSafety Skills Development for Staff	14
INCIDENT REPORTING	15
Incident Reporting	15
INTERNET ACCESS	16
Managing the Internet	16
Internet Use	16
Infrastructure	16
PARENTAL INVOLVEMENT	18
PASSWORDS AND PASSWORD SECURITY	19
Passwords	19
Password Security	19
SAFE USE OF IMAGES	20
Taking of Images and Film	20
Consent of Adults Who Work at the School	20
Publishing Pupil’s Images and Work	20
Storage of Images	21

Webcams and CCTV	21
Video Conferencing	21
SCHOOL ICT EQUIPMENT INCLUDING PORTABLE & MOBILE ICT EQUIPMENT & REMOVABLE MEDIA	22
School ICT Equipment within School	22
Portable & Mobile ICT Equipment	22
Mobile Technologies	23
Personal Mobile Devices (including phones)	23
TELEPHONE SERVICES	24
School Mobile Phones	24
REVIEWING THIS POLICY	25
Review Procedure	25
CURRENT LEGISLATION	26
Acts Relating to Monitoring of Staff eMail	26
Other Acts Relating to eSafety	26
Acts Relating to the Protection of Personal Data	28

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 Bow Community Primary School, we understand the responsibility to educate our pupils 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.

Schools hold 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 the school.

Everybody in the 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 pupils) are inclusive of both fixed and mobile internet; technologies provided by the school (such as PCs, laptops, personal digital assistants (PDAs), tablets, webcams, whiteboards, voting systems, digital video equipment, etc); and technologies owned by pupils and staff, but brought onto school premises (such as laptops, mobile phones, camera phones, PDAs and portable media players, etc).

Monitoring

ICT authorised staff may inspect any ICT equipment owned or leased by the School at any time without prior notice. Authorisation is given by the Headteacher and/or the Chair of Governors. Written proof of authorisation should be retained for the avoidance of future doubt or dispute.

ICT authorised staff may, without prior notice, access the e-mail account 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 must comply with the Data Protection Act 2018, 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, volunteer or pupil may result in the temporary or permanent withdrawal of School ICT hardware, software or services from the offending individual.

Any policy breach may be grounds for disciplinary action in accordance with the School Disciplinary Procedure or, where appropriate, or Probationary Service Policy.

Policy breaches may also lead to criminal or civil proceedings.

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 ICT Co-ordinator or Headteacher. Additionally, all security breaches, lost/stolen equipment or data (including remote access SecureID tokens and PINs), virus notifications, unsolicited emails, misuse or unauthorised use of ICT and all other policy non-compliance must be reported to the ICT Co-ordinator or Headteacher.

Acceptable Use Agreement: Pupils

Primary Pupil Acceptable Use Agreement / eSafety Rules

- I will only use ICT in school for school purposes.
- I will make sure that all ICT contact with other children and adults is responsible, polite and sensible.
- I will not deliberately look for, save or send anything that could be unpleasant or nasty. If I accidentally find anything like this I will tell my teacher immediately.
- I will not give out my own details such as my name, phone number or home address. I will not arrange to meet someone unless this is part of a school project approved by my teacher and a responsible adult comes with me.
- I will be responsible for my behaviour when using ICT because I know that these rules are to keep me safe.
- I will support the school approach to online safety and not deliberately upload or add any images, video, sounds or text that could upset any member of the school community
- I know that my use of ICT can be checked and that my parent/ carer contacted if a member of school staff is concerned about my eSafety.

Dear Parent/ Carer

ICT including the internet, e-mail and mobile technologies, etc has become an important part of learning in our school. We expect all children to be safe and responsible when using any ICT.

Please read and discuss these eSafety rules with your child and return the slip at the bottom of this page. If you have any concerns or would like some explanation please contact your class teacher or the headteacher at school.

✂-----

Parent/ carer signature

We have discussed this and(child name) agrees to follow the eSafety rules and to support the safe use of ICT at Bow Community Primary School.

Parent/ Carer Signature

Class Date

Acceptable Use Agreement: Staff, Governors and Visitors

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

ICT (including data) and the related technologies such as e-mail, the internet and mobile devices are an expected part of our daily working life in school. This 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 Lesley Hodgson, Headteacher or Chris Johnston, ICT co-ordinator.

- I will only use the school's email / Internet / Intranet / Learning Platform 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 pupils and staff are compatible with my professional role.
- I will not give out my own personal details, such as mobile phone number and personal e-mail address, to pupils.
- I will only use the approved, secure e-mail system(s) for any school business.
- I will ensure that personal data (such as data held on MIS software) 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. Personal or sensitive data taken off site must be encrypted.
- I will not install any hardware or software without permission of the ICT co-ordinator or Headteacher
- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.
- Images of pupils 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 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 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 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 e-Safety and Data Security policies and help pupils to be safe and responsible in their use of ICT and related technologies.

User Signature

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

Signature Date

Full Name(printed)

Job/Role title

Computer Viruses

- All files downloaded from the Internet, received via e-mail or on removable media (e.g. USB stick, CD) must be checked for any viruses using school provided anti-virus software before using them
- Users (staff, volunteers, governors or pupils) must never interfere with any anti-virus software installed on school ICT equipment being used.
- Anyone who suspects there may be a virus on any school ICT equipment, must stop using the equipment and contact the ICT co-ordinator immediately. The ICT co-ordinator will advise what actions need to be taken and be responsible for advising others that need to know

e-Mail

The use of e-mail within most schools is an essential means of communication. 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 pupil based, within school or international.

Managing e-Mail

- The school gives all teaching staff their own e-mail account to use for all school business as a work based tool This is to minimise the risk of receiving unsolicited or malicious e-mails and avoids the risk of personal profile information being revealed
- 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 pupils or 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 are advised to cc. the Headteacher where appropriate
- Pupils may only use school approved accounts on the school system and only under direct teacher supervision for educational purposes
- E-mails created or received will be subject to disclosure in response to a request for information under the Freedom of Information Act 2000 or under a subject access request. All account holders must therefore actively manage their 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 forwarding of chain letters is not permitted in school.
- Staff must inform the ICT Co-ordinator or Headteacher if they receive an offensive e-mail
- The use of Hotmail, BT Internet, AOL or any other Internet based webmail 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
- Keep the number and relevance of e-mail recipients, particularly those being copied, to the minimum necessary and appropriate
- 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 advertising

Receiving e-Mails

- All account holders should check their e-mail regularly
- Account holders should never open attachments from an untrusted source; Consult the ICT Co-ordinator first.

e-mailing Personal, Sensitive, Confidential or Classified Information

- Before using e-mail, account holders should 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
- The use of Hotmail, BT Internet, AOL or any other Internet based webmail service for sending e-mail containing sensitive information is not permitted
- Where the conclusion is that e-mail must be used to transmit such data:
 - Obtain express consent from the head teacher to provide the information by e-mail
 - Exercise caution when sending the e-mail and always follow these checks before releasing the e-mail:
 - 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 any body/person whose details have not been separately verified (usually by phone)
- 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:

- Constabulary
- Partnership Trust

Equal Opportunities

Pupils with Additional Needs

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

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

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 named ICT co-ordinator in this school is Chris Johnston, who has been designated this role by the senior leadership team. All members of the school community have been made aware of who holds this post. It is the role of the ICT co-ordinator to keep abreast of current issues and guidance through organisations such as SWGfL, Becta, CEOP (Child Exploitation and Online Protection) and Childnet.

Senior Management and Governors are updated by the Headteacher or the ICT co-ordinator and all governors have an understanding of the issues and strategies at 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 pupils, 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/pupil discipline (including the anti-bullying) policy and PSHE

eSafety in the Curriculum

ICT and online resources are increasingly used across the curriculum. We believe it is essential for eSafety guidance to be given to the pupils on a regular and meaningful basis. eSafety is embedded within our curriculum and we continually look for new opportunities to promote eSafety.

- The school has a framework for teaching ICT and internet skills. Teaching of ICT within school comes from the Government's National Curriculum Policy (2002).
- On an annual basis, during anti-bullying week, staff tackle e-safety, looking at how to behave on the internet, what you should do if you see something you don't like, as well as teaching them about restricted sites. They learn about CEOPS, as well as mobile phone safety and about cyber-bullying. We follow the recommendations of CEOPS
- We include e-safety in assemblies during the year, it is also included in our PSHE lessons when appropriate and we have posters up, behind the door in the ICT suite, with the Do's and Don'ts on

eSafety Skills Development for Staff

- New staff receive information on the school's acceptable use policy as part of their induction
- All staff have been made aware of 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.
- All staff are encouraged to incorporate eSafety activities and awareness within their curriculum areas

Incident Reporting

Incident Reporting

Any security breaches or attempts, loss of equipment and any unauthorised use or suspected misuse of ICT must be reported to the ICT co-ordinator, who will record them within the e-Safety Incident Log.

Some incidents may need to be recorded in other places, such as the e-Safety log, if they relate to a bullying or racist incident.

Actions to contain and manage the incident will be determined by the ICT co-ordinator with the support of the Headteacher, staff, governors or other agencies (e.g. County Council) as required.

On a termly basis, the Headteacher and a nominated Governor will review the Incident Log, to determine any policy or strategic actions required to prevent or contain future Incidents.

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 **Grid for Learning** (SWGfL) is logged and the logs are randomly but regularly monitored. Whenever any inappropriate use is detected it will be followed up.

Managing the Internet

- Pupils 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 pupils
 - 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

- Users must not post personal, sensitive, confidential or classified information or disseminate such information in any way that may compromise its intended restricted audience
- Users must not reveal names of colleagues, pupils or any other confidential information on any social networking site or blog
- On-line gambling or gaming is not allowed

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

Infrastructure

- The Local Authority has a monitoring solution via the 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>

- Bow Community Primary School is aware of its responsibility when monitoring staff communication under current legislation and takes into account; Data Protection Act 2018, The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, Regulation of Investigatory Powers Act 2000, Human Rights Act 1998
- Staff and pupils are aware that school based email and internet activity can be monitored and explored further if required
- The school does not allow pupils access to internet logs
- 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
- Staff using personal removable media (e.g. USB sticks or CDs) 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.

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 asked to read through and sign acceptable use agreements on behalf of their child on admission to school
- 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)
- The school disseminates information to parents relating to eSafety where appropriate in the form of;
 - Information and celebration evenings
 - Posters
 - Website
 - Newsletter items

Passwords and Password Security

Passwords

- Account holders should always use their own personal passwords to access computer based services
- Account holders must make sure they enter their personal passwords each time they logon. Do not include passwords in any automated logon procedures
- Account holders should change temporary passwords at first logon
- Passwords must be changed whenever there is any indication of possible system or password compromise
- Passwords or encryption keys must not be recorded on paper or in an unprotected file
- Passwords may only be disclosed 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

Password Security

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

- All users read and sign an Acceptable Use Agreement to demonstrate that they have understood the school's e-safety Policy
- Users are provided with an individual network, email, Learning Platform and Management Information System (where appropriate) log-in username.
- Pupils 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, MIS systems and/or Learning Platform, 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.

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.

- With the written consent of parents (on behalf of pupils) and staff, the school permits the appropriate taking of images by staff and pupils with school equipment
- Staff are not usually permitted to use personal digital equipment, such as mobile phones and cameras, to record images of pupils, this includes when on field trips. However with the express permission of the Headteacher, images can be taken provided they are transferred as soon as possible and solely to the school's network and deleted from the staff device

Consent of Adults Who Work at the School

- Permission to use images of all staff who work at the school is sought on induction and a copy is located in the personnel file

Publishing Pupil'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 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 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. Consent has to be

given by both parents in order for it to be deemed valid.

Pupils' names will not be published alongside their image and vice versa. E-mail and postal addresses of pupils will not be published. Pupils' full names will not be published unless parental consent has been sought and given.

Storage of Images

- Images/ films of children are stored on the school's network
- Pupils 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 pupils within the confines of the school network/ Learning Platform
- The ICT Co-ordinator has the responsibility of deleting the images when they are no longer required, or the pupil has left the school

Webcams and CCTV

- We do not use publicly accessible webcams in school
- Webcams in school are only ever used for specific learning purposes, i.e. monitoring birds' eggs and never using images of children or adults

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 with end-points outside of the school or the learning community. A school Video Conferencing Policy will apply.
- All pupils must be supervised by a member of staff when video conferencing
- No part of any video conference is recorded in any medium without the consent of those taking part

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

School ICT Equipment within School

- Staff are responsible for any activity undertaken on the school's ICT equipment, including mobile and portable equipment whilst on school premises
- Staff must 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
- Staff must save data on a frequent basis to the school's network drive. Personal or sensitive data should not usually be stored on the local drives of desktop PCs. If it is necessary to do so the local drive must be encrypted
- Privately owned ICT equipment should not be used on a school network
- On termination of employment, resignation or transfer, staff must return all ICT equipment. Staff must also provide details of all system logons so that they can be disabled
- 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 should 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 the car before starting the journey
- Staff should synchronise all locally stored data, including diary entries, with the central school network server on a frequent basis
- Staff must ensure that 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 co-ordinator or Head Teacher and be fully licensed

- 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

Mobile Technologies

Many emerging 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. Emerging technologies will be examined for educational benefit and the risk assessed before use in school is allowed. Our 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 and use for school on field trips and similar circumstances. Under no circumstances does the school allow a member of staff to contact a pupil or parent/ carer using their personal device
- Pupils, visitors and volunteers are discouraged from bringing personal mobile devices/phones to school.
- Where visitors and volunteers do bring personal mobile devices into school, they are either subject to standard DBS checks or accompanied by a checked member of staff. All volunteers receive training in safeguarding, including the appropriate use of media and mobile devices.
- Where pupils must bring personal mobile devices into school, the device must be handed to staff in the school office for safe storage during the school day.
- The school is not responsible for the loss, damage or theft of any personal mobile device
- The sending of inappropriate text messages 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

Telephone Services

School Mobile Phones

- Staff are responsible for the security of the school mobile phone allocated to them.
- The loss or theft of the school mobile phone equipment must be reported immediately
- The school remains responsible for all call costs until the phone is reported lost or stolen
- Staff must read and understand the user instructions and safety points relating to the use of the school mobile phone prior to using it
- School SIM cards must only be used in school provided mobile phones
- At the discretion of the Head Teacher, Staff may be required to reimburse the school for the cost of any personal use of a school mobile phone.

Reviewing this Policy

Review Procedure

This policy will be reviewed every 2 years, and consideration given to the implications for future whole school development planning

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

Current Legislation

Acts Relating to Monitoring of Staff eMail

Data Protection Act 2018

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.

<https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted>

The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000

<http://www.hmso.gov.uk/si/si2000/20002699.htm>

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 is 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 person's 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 their 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 2018

<https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted>

The Freedom of Information Act 2000

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

General Data Protection Regulation 2018

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