



Bentfield Primary School

ICT and E-Safety Policy

Aim

Bentfield Primary school, through this policy, wishes to provide guidelines under which staff and students should feel confident about the use of ICT and related technologies in the delivery and enhancement of teaching and learning.

Objectives

- To ensure that students and staff use ICT and related technologies safely and securely.
- To ensure that students' learning is enhanced to maximum extent.
- To safeguard students' rights for equal opportunity to participate and use ICT.
- To ensure that responsibilities for staff are clear and that required formalities and agreements are adhered to.
- To ensure that staff and pupils are protected from harm that may occur through use of ICT resources within school.
- To provide staff, pupils and parents with guidance on how to keep themselves and others safe when using online resources at school and at home.

Introduction

ICT is an essential resource to support learning and teaching, as well as playing an important role in the everyday lives of 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 as well as providing a coherent, sequential and thorough computing curriculum.

ICT 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. All users need to be aware of the range of risks associated with the use of ICT related technologies.

Both this policy and the Acceptable Use Agreement – found in the Staff Code of Conduct policy – (for all staff, governors, visitors and students) include 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 privately owned by students and staff, but brought onto school premises.

Monitoring

Authorised ICT staff may inspect any ICT equipment owned or leased by the school at any time without prior notice. ICT authorised staff may monitor, intercept, access, inspect, record and disclose e-mails, instant messaging, internet/intranet use and any other electronic communications involving its employees or contractors, without consent, to the extent permitted by law. This includes monitoring via our school web filtering to monitor blocked websites that have been attempted to be visited. This may be to confirm or obtain school business related information; to confirm or investigate compliance with school policies, standards and procedures; to ensure the effective operation of school ICT; for quality control or training purposes; to comply with a Subject Access Request under the Data Protection Act 2018, or to prevent or detect crime.

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

All monitoring, surveillance or investigative activities are conducted by ICT authorised staff and comply with the Data Protection Act 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.

All internet activity is logged by the school's internet provider. These logs may be monitored by authorised ECC staff.

Breaches

A breach or suspected breach of policy by a school employee, contractor or student may result in the temporary or permanent withdrawal of school ICT hardware, software or services from the offending individual. Any policy breach is grounds for disciplinary action in accordance with the school disciplinary procedure. In extreme cases, 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 designated member of SLT with responsibility for ICT and E-Safety. Where concerns with use of ICT equipment are a safeguarding concern, the DSL or a Deputy DSL will be informed via My Concern and verbally if appropriate.

Computer Viruses

- All files downloaded from the Internet, received via e-mail or on removable media (e.g. memory stick, CD) must be checked for any viruses using school provided anti-virus software before using them. Training on how to do this is available from the network support team.
- Staff should never interfere with any anti-virus software installed on any school ICT equipment that they use.
- If staff suspect there may be a virus on any school ICT equipment, they should stop using the equipment and contact the ICT network support team immediately.

Data Security

The handling of secured data is everyone's responsibility – whether they are an employee, consultant, software provider or managed service provider. In extreme cases, failing to apply appropriate controls to secure data could amount to gross misconduct or even legal action.

- The school gives relevant staff access to its Management Information System and Network, with a unique ID and password. It is the responsibility of everyone to keep these passwords secure (See password section below).
- All staff should keep all school related data secure. This includes all personal, sensitive, confidential or classified data.
- Staff should avoid leaving any portable or mobile ICT equipment or removable storage media in unattended vehicles. Where this is not possible, staff should keep it locked.
- Staff should always carry portable and mobile ICT equipment or removable media as hand luggage, and keep it under their control at all times.
- It is the responsibility of individual staff to ensure the security of any personal, sensitive and confidential information contained in documents copied, scanned or printed.

Access to the network

Access to the curriculum network is password controlled; all staff members have their own username and password. Pupils have their own usernames (and passwords in KS2), though they have restricted access to their own allocated folder and relevant software. Access to the administrative network is limited to the Office Manager, Office Staff, and Headteacher.

Passwords

- Staff should change passwords whenever there is any indication of possible system or password compromise.
- Staff should not record passwords or encryption keys on paper or in an unprotected file.
- Staff should disclose their personal password to the ICT network support staff when necessary, and never to anyone else.
- User ID and passwords for staff and students who have left the school will always be removed from the system.

Strategic Overview

The senior member of staff with designated responsibility for ICT should be familiar with information risks and the school's response. It is this person's responsibility to minimise any risks present. It is also this person's responsibility to understand:

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

These responsibilities can be delegated as appropriate to suitably appointed staff.

Disposal of Redundant ICT Equipment Policy

- All redundant ICT equipment will be disposed of through an authorised agency or authority.
- All redundant ICT equipment that may have held personal data will have the storage media wiped to ensure the data is irretrievably destroyed or be physically destroyed (by the network support team).
- The school will maintain a comprehensive inventory of all its ICT equipment including a record of disposal.
- Any redundant ICT equipment being considered for sale/gift will hold a valid PAT certificate.

E-Mail

Email is used at Bentfield Primary School for the following reasons:

- Staff to staff communication
- Liaising with outside organisations regarding visits, trips etc
- Receiving emails from educational websites
- Signing up to relevant educational websites
- Communication with parents – this is done through class email addresses by class teachers, Arbor, or the school admin account.

Where communication contains sensitive or critical such that if the contents were disclosed or modified by an unauthorised person it could cause embarrassment, distress or financial loss, staff 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. Where staff conclude that e-mail must be used to transmit such data:

- They should exercise caution when sending the e-mail and always follow these checks before releasing the e-mail:
 - Staff should verify the details, including accurate e-mail address, of any intended recipient of the information.
 - Staff should verify (by phoning) the details of a requestor before responding to e-mail requests for information.
 - Staff should not copy or forward the e-mail to any more recipients than is absolutely necessary.
- Staff should not send the information to anybody/person whose details they have been unable to separately verify (usually by phone).
- Staff should not identify such information in the subject line of any e-mail.
- Staff should request confirmation of safe receipt.

E-Safety - Roles and Responsibilities

It is the role of the designated member of SLT with responsibility for E-Safety and ICT to keep abreast of current issues and guidance through organisations such as the LA, CEOP (Child Exploitation and Online Protection) and Childnet.

Senior Management and Governors are updated by the Head/E-Safety Co-ordinator/**DSL** and all governors have an understanding of the issues and strategies at the school in relation to local and national guidelines and advice.

This policy, supported by the school's code of conduct for staff, governors, visitors and students, is to protect the interests and safety of the whole school community. It is linked to the following school policies: child protection, code of conduct, health and safety, home school agreements, and behaviour.

E-Safety in the Curriculum

ICT and online resources are used across the curriculum. It is essential for E-Safety guidance to be given to the students on a regular and meaningful basis. We use a measured approach to web filtering to ensure that it does not block access to websites that will be useful for the children's learning across the whole curriculum.

- The school has a framework for teaching internet skills in relevant computing lessons.
- The school provides opportunities within PSHE and computing to teach about E-Safety.
- In KS1, pupils are taught about e-safety in a half-term unit of work. In KS2, pupils are taught about e-safety in their first computing lesson of each half-term.
- In addition to lessons taught formally within the computing and PSHE curricula, assemblies will take place about e-safety through the school year and individual classes will teach children about any specific issues surrounding e-safety that occur and are relevant to them. This can include teaching about e-safety issues that have come to light from their use of online communications outside of school.
- Students are taught about copyright and respecting other people's information, images, etc. through discussion, modelling and activities.

Students are aware of the impact of cyberbullying and know how to seek help if they are affected by any form of online bullying i.e. parent/carer, teacher/trusted staff member, an organisation such as Childline or CEOP report abuse button.

Social Networking

- All students are advised to be cautious about the information given by others on sites, for example users not being who they say they are.
- Students are taught to avoid placing images of themselves (or details within images that could give background details) and to consider the appropriateness of any images they post due to the difficulty of removing an image once online.
- Students are always reminded to avoid giving out personal details on such sites which may identify them or where they are (full name, address, mobile/ home phone numbers, school details, IM/ e-mail address, specific hobbies/ interests).
- Students are advised to set and maintain profiles on such sites to maximum privacy and deny access to unknown individuals.
- Students are encouraged to be wary about publishing specific and detailed private thoughts online.
- Students are asked to report any incidents of cyberbullying to the school.
- These skills are taught through the computing and PSHE curriculum.

E-Safety 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 E-Safety 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 E-Safety activities and awareness within their curriculum areas.

E-Safety Incident Log

Incidents relating to E-Safety should be recorded on the school MyConcern safeguarding software.

Inappropriate Material

- Accidental access to inappropriate materials must be immediately reported to the designated SLT member responsible for E-Safety and, if appropriate, the DSL or a Deputy DSL.
- Deliberate access to inappropriate materials by any user will be logged; investigation by the Headteacher/LA, immediate suspension, possibly leading to dismissal and involvement of police for very serious offences.
- Web filtering via School's Broadband will be used to block access to inappropriate materials. If inappropriate materials are still accessed, this will be reported to the designated member of SLT responsible for E-safety and DSL, who will work with the ICT technician to use our web filtering service to block access to this.

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 internet is logged by Essex County Council and the logs are randomly but regularly monitored by county representatives.

Managing the Internet

- Students should have (supervised) access to Internet resources (where reasonable) through the school's fixed and mobile internet technology.
- Staff should preview any recommended sites before use.
- If Internet research is set for homework, specific sites will be suggested that have previously been checked by the teacher.
- 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

- Use of the internet by staff and pupils is set out within the staff code of conduct and in the acceptable use agreement for pupils.

Filters

- School internet access is controlled through the School's Broadband filtering service
- The DSL is responsible for ensuring that web filtering is appropriate for the school, blocking harmful content, but not blocking content which will be useful to children's learning across the curriculum.
- The Strategic Leader of ICT Technologies is aware of their 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 and the Human Rights Act 1998.
- Staff and students are aware that school based e-mail and internet activity can be monitored and explored further if required.
- The school does not allow students access to internet logs.
- If staff or students discover an unsuitable site, the screen must be switched off/ closed and the incident reported immediately to the ICT leads or teacher as appropriate.
- It is the responsibility of the school, by delegation to the network manager, to ensure that anti-virus protection is installed and kept up-to-date on all school machines.
- Students and staff using personal removable media are responsible for measures to protect against viruses, for example making sure that additional systems used have up-to-date virus protection software. It is not the school's responsibility nor the network manager's to install or maintain virus protection on personal systems. If students wish to bring in work on removable media, it should be given to an ICT technician or the teacher for a safety check first. Sensitive data must never be taken off site unless it is encrypted. Memory sticks can be encrypted by the ICT technician if required.
- If there are any issues related to viruses or anti-virus software, the network manager should be informed by phone call or e-mail.
- Web filtering will be monitored on an ongoing basis. This includes any concerns with what can or cannot be accessed as and when they occur, as well as termly checks to ensure filtering is appropriate.

Parental Involvement

- It is essential for parents/carers to be fully involved with promoting E-Safety both in and outside school and also to be aware of their responsibilities. The school regularly consults and discuss E-Safety 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 E-Safety where appropriate in the form of;
 - Information evenings
 - Website postings
 - Newsletter items
 - Letters to parents of specific classes where e-safety incidents have occurred

Protecting Personal, Sensitive, Confidential and Classified Information

- Staff should ensure that any school information accessed from your own PC or removable media equipment is kept securely.
- Staff should ensure they lock their machine before moving away from their computer during the normal working day to prevent unauthorised access.
- Staff should ensure the accuracy of any personal, sensitive, confidential and classified information they disclose or share legitimately with others.
- Staff should ensure that personal, sensitive, confidential or classified information is not disclosed to any unauthorised person.
- Staff should ensure the security of any personal, sensitive, confidential and classified information contained in documents you copy, scan or print.
- Staff must not post personal, sensitive, confidential, or classified information on the internet, or disseminate such information in any way that may compromise its intended restricted audience.
- Staff should ensure hard copies of data are securely stored and disposed of (shredded) after use.

Using Removable Media

- Staff should store all removable media securely.
- Staff should securely dispose of removable media that may hold personal data.
- Staff should always encrypt all files containing personal, sensitive, confidential or classified data (training on this can be obtained from the network support team).
- Staff should ensure hard drives from machines no longer in service are removed and stored securely or wiped clean via the network support team.

Remote Access

- Staff are responsible for all activity via the remote access facility.
- Staff should only use equipment with an appropriate level of security for remote access (e.g. staff should not use machines in a public place such as an internet café).
- Staff should protect school information and data at all times, including any printed material produced while using the remote access facility. Staff should take particular care when access is from a non-school environment.

Safe use of Images and Film

Digital images are easy to capture, reproduce and publish and, therefore, misuse. Staff should 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 consent of parents (on behalf of students) and staff, the school permits the appropriate taking of images by staff and students with school equipment.

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 Students' Images and Work

On a student'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 display material that may be used in the school's communal areas
- In the school prospectus and other printed publications that the school may produce for promotional purposes
- In display material that may be used in external areas, i.e. exhibition promoting the school
- General media appearances, e.g. local/ national media/ press releases sent to the press highlighting an activity (sent using traditional methods or electronically)
- Videoing for in house purposes, e.g. school productions or drama/PE lessons
- This consent is considered valid for the entire period that the child attends this school.
- Parents/ carers may withdraw permission, in writing, at any time.
- E-mail and postal addresses of students will not be published.

School ICT Equipment

- Staff and students are responsible for any activity undertaken on the school's ICT equipment provided to them.
- Staff should not allow visitors to use their ICT hardware in conjunction with the school network without consultation with the ICT network support team.
- Staff should ensure that all ICT equipment that is used is kept physically secure.
- Staff should 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 should save their data on a frequent basis to the school's cloud based network. Staff are responsible for the backup and restoration of any data that is not held on the school's network drive.
- Personal or sensitive data should not be stored on the local drives of desktop PCs or laptops.
- Privately owned ICT equipment including personal laptops should not be used on a school network unless with express permission from the Strategic Leader of ICT. Any privately owned ICT (or ICT related) equipment must be subject to the usual rules and regulations surrounding the protection of children and e-safety as laid out in this and other policies or guidance.
- It is the responsibility of the staff to ensure that no personal, sensitive, confidential or classified information is disclosed to any unauthorised person.
- 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

- 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 cloud based network, and not kept solely on a laptop. Any equipment where personal data is likely to be stored must be encrypted and/or password protected.
- Staff should ensure that equipment is 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 ensure portable and mobile ICT equipment is made available as necessary for anti-virus updates and software installations, patches or upgrades.
- The installation of any applications or software packages must be authorised by the ICT network support team and fully licensed. All other packages will be removed.
- In areas where there are likely to be members of the general public, portable or staff must not leave mobile ICT equipment unattended and, wherever possible, kept out of sight.
- Portable equipment must be transported in its protective case.

Mobile Technologies

- The school allows staff to bring in personal mobile phones and devices for their own use, however they must follow the school's use of mobile phones policy.
- Students are allowed to bring personal mobile devices/phones to school but must not use them during the school day. They are to be handed to their class teacher and collected at the end of the day. They will be kept in a secure location by the class teacher during the day.
- The school is not responsible for the loss, damage or theft of any personal mobile device.

School Provided Mobile Devices (including phones)

The school may provide a mobile phone for specific purposes, e.g. residential visits, school trips, or use by breakfast/kids club.

- The sending of inappropriate text messages between members of the school community is not allowed.
- Permission must be sought before any image or sound recordings are made.

Devices brought in from home

- Staff may bring their own mobile devices into school from home. These are not expected to be used for any school-based activities and, as such, will not be connected to the school network WiFi except in exceptional circumstances approved by the Headteacher. Expectations of staff use of mobile devices in school is set out in staff code of conduct.
- Students who have permission to walk to and from school themselves are permitted to bring their mobile phones into school. These should be turned off at the school gate and not turned on again until they have left the school site. Phones are handed in to teachers as soon as students reach the classroom and are kept securely by the class teacher until they are handed back at the end of the school day. Therefore, these devices are not used during the school day.
- Teachers, where they feel it is appropriate, may allow pupils to bring in other mobile devices as part of a class reward. Devices brought in are not permitted to be connected to school WiFi and students are not

permitted to bring in devices with other internet connection e.g. 4G/5G. All devices are checked for this by the class teacher before any use in school. Class staff will monitor the use of these devices very closely to ensure that games played on these are age-appropriate ie. U or PG rated.

Systems and Access

- Staff are responsible for all activity on school systems carried out under any access/account rights assigned to you, whether accessed via school ICT equipment or your own PC (which is not recommended).
- Staff should not allow any unauthorised person to use school ICT facilities and services that have been provided to them.
- Staff should use only their own personal logons, account IDs and passwords and must not allow them to be used by anyone else.
- Staff should ensure that they logoff from the PC completely when they are going to be away from the computer for a longer period of time.
- Staff must not intentionally introduce or propagate viruses.
- It is imperative that staff do not access, load, store, post or send from school ICT any material that is, or may be considered to be, illegal, offensive, libellous, pornographic, obscene, defamatory, intimidating, misleading or disruptive to the school or may bring the school or ECC into disrepute. This includes, but is not limited to, jokes, chain letters, files, e-mails, clips or images that are not part of the school's business activities; sexual comments or images, nudity, racial slurs, gender specific comments, or anything that would offend someone on the basis of their age, sexual orientation, religious or political beliefs, national origin, or disability (in accordance with the Sex Discrimination Act, the Race Relations Act and the Disability Discrimination Act).
- Any information held on school systems, hardware or used in relation to school business may be subject to The Freedom of Information Act.
- Where necessary, staff should obtain permission from the owner or owning authority and pay any relevant fees before using, copying or distributing any material that is protected under the Copyright, Designs and Patents Act 1998.
- It is essential that any hard drives which may have held personal or confidential data are 'scrubbed' in a way that means the data can no longer be read. It is not sufficient to simply delete the files or reformat the hard drive (this to be done by the network support team).

Bentfield Primary School and its Governing Body is committed to ensuring consistency of treatment and fairness and will abide by all relevant equality legislation.

Teaching and Learning – Computing Curriculum

Computing lessons are taught discretely each week across years 1-6. Each class focuses on a specific type of software each half-term, building skills within the software as set out in our computing curriculum. The software used includes coding, word processing, communicating, illustrating and mapping. All lessons build towards the pupils achieving the curriculum objectives set out in the Primary National Curriculum.

Teachers' planning in terms of computing and e-safety is differentiated to meet the range of needs in any class, including: those children who may need extra support, those who are in line with national expectations and those working above national expectations for children of their age.

A wide range of styles are employed to ensure all children are sufficiently challenged:

- Children may be required to work individually, in pairs or in small groups according to the nature or activity of the task
- Different pace of working
- Different groupings of children - groupings may be based on ability either same ability or mixed ability
- Different levels of input and support
- Different outcomes expected

Teaching and Learning – ICT across the curriculum

The use of ICT resources in lessons can enhance pupils' learning. Within the classroom at Bentfield Primary School we use a variety of methods to support our teaching using ICT. This includes:

- Use of interactive Sahara boards
- Screen mirroring using iPads
- Using class set of iPads e.g. for educational games, activities or research purposes
- Adapting learning for children with SEND e.g. typing using a laptop, eye gazes

The use of desktop computers in the ICT suite can also enhance pupils' learning. This is done in a variety of ways including:

- Using the internet for research purposes
- Using specific software for interventions
- Putting together presentations or displays using computer software

Early Years

It is important in the foundation stage to give children a broad, play-based experience of IT in a range of contexts, including outdoor play. IT is not just about computers. Early years control and language skills through opportunities to 'paint' on the whiteboard or programme a toy. Recording devices can support children to develop their communication skills. This is particularly useful with children who have English as an additional language.

Monitoring of teaching and learning in computing

The Computing coordinator is responsible for the quality of teaching and learning in computing lessons through the monitoring and feedback cycle, which includes lesson dips, and pupil voice. The computing coordinator will use this information to plan for further developments within the subject, including individual and whole staff training opportunities. The use of ICT across all other curriculum subjects to enhance teaching and learning is monitored by the subject coordinators.

Equal Opportunities

The National Curriculum states that, "All pupils, regardless of race, class or gender, should have the opportunity to develop computing capability." It is our policy to ensure this by:

- ensuring all children follow the scheme of work for computing
- keeping a record of children's computing use to ensure equal access and fairness of distribution of computing resources

- providing curriculum materials and software which are in no way class, gender or racially prejudice or biased

Home Learning

Where pupils are unable to attend school, but are well enough to complete work, the class teacher will provide work for those pupils to complete at home. This will be set using one of the following platforms:

- Purple Mash
- Class email
- Espresso Coding
- Times Tables Rockstars
- Maths frame
- Spelling frame
- Microsoft Teams

All completed work can be submitted to the class teacher for feedback.

Pupils will be kept safe when using online software for completing schoolwork at home by:

- Using individual logins provided by the school
- Having their class teacher monitor their usage
- Class emails being available for parents to contact school about any issues that occur
- Any tasks that involve searching the internet, will have recommended websites that have been checked by the class teacher beforehand

If pupils do not have access to appropriate ICT resources at home, the school will provide a laptop so that they are able to complete any remote work set.

Appendix 1

Acts Relating to Monitoring of Staff E-Mail

Data Protection Act 1998

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

<http://www.hmso.gov.uk/acts/acts1998/19980029.htm>

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.

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

Human Rights Act 1998

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

Acts Relating to E-Safety

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.

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
- unauthorised access, as above, in order to commit a further criminal act (such as fraud)
- impair the operation of a computer or program

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 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

Information Commissioner Website <http://www.ico.gov.uk/>

Appendix 2



Bentfield Primary School **ICT Code of Conduct for Pupils**

The school has installed computers, iPads and laptops with Internet access to help your learning. These rules will keep you safe.

- You are responsible for your own behaviour on the internet, just as you are anywhere else in school. This includes the materials you choose to access and the language you use.
- Always ask permission from a member of staff before using the Internet.
- Do not access other people's files without permission.
- Use your own login to access the computers, not another child's. You may share a computer with another pupil if they are present.
- Only use the computers for schoolwork.
- Do not bring in memory sticks from outside school unless you have been given permission.
- Never give out any addresses, telephone numbers or arrange to meet someone unless your parent or teacher know and have given you permission.
- Do not give names of friends or family members to anybody on the Internet.
- Do not go into any 'chat rooms' (These should already be blocked).
- Do not deliberately seek out any inappropriate or offensive materials.
- If you see any unpleasant material, or have unsuitable messages sent to you, turn off the monitor and tell a member of staff immediately (DO NOT turn off the actual computer itself).
- Uploading or downloading of files or software to or from the internet is not permitted.
- The school may check your computer files and may monitor the Internet sites that you visit.
- If you consistently fail to comply with these expectations you will be warned, and subsequently, may be denied access to the internet resources.

Appendix 3

ICT Acceptable Use Policy – Part of the Code of Conduct

Introduction

ICT (including data) and the related technologies such as computers, email, the internet and mobile devices are an expected part of daily working life in school and the use of electronic communication and resources is encouraged.

All members of the school community are expected to use ICT responsibly and to comply with all applicable laws, policies and procedures, and with normal standards of professional and personal courtesy and conduct.

This policy is designed to ensure that all workers are aware of their professional responsibilities when using any form of ICT.

Failure to follow this policy may result in the withdrawal of access to school computers, email and internet and/or to disciplinary action, depending on the circumstances of the case.

Technology and the law change regularly and this policy will be updated as and when necessary. Workers will be informed when the policy has changed but it is their responsibility to read the latest version of this document.

Use of School Equipment/Networks

Computers, Mobile Phones and other devices provided by the school are loaned to individuals to support their professional responsibilities and must be used in accordance with this policy.

Workers are responsible for the safe and proper use, care and security of equipment and systems provided. Devices must be secured appropriately especially when leaving the school premises (i.e. not left unattended) and protected from unauthorised access or use (i.e. not accessed by family members). Any loss, damage or unauthorised access must be reported immediately.

Workers must not use school equipment, networks or system to access, download, send or receive, store, create, copy or distribute any material which may be malicious, illegal, libellous, immoral, dangerous or offensive (this includes but is not limited to pornographic, sexual, violent or criminal content and racist, sexist, or otherwise discriminatory material).

Any appropriate and authorised electronic communication with pupils must be through official school network, channels, systems and on school equipment.

Use of Email

School business must always be conducted through official email addresses, which must be secured with password controls. Workers should respond to emails during working hours in a timely and appropriate fashion.

Email should be treated like any other form of written communication and, as such, the content should be appropriate and accurate and data protection compliant.

Extreme care must be taken with attachments from third parties, particularly unidentified third parties, as these may contain viruses.

Email must not be used to receive, send or forward messages that are defamatory, obscene or otherwise inappropriate. If such an email is received, whether unwittingly or otherwise and from whatever source, this must not be forwarded to any other address and must be reported immediately.

Reasonable access and use of the internet/intranet and email facilities is available to recognised representatives of professional associations' i.e. union officers for the performance of their official duties and activities.

Social Networks

Social networking applications include but are not limited to:

- Blogs
- Online discussion forums, for example Facebook;
- Media sharing services for example YouTube;
- Professional networking sites, for example Linked In
- 'Micro-blogging' application for example Twitter

Where the school operates official networking sites, these must be managed and used in accordance with this policy. This includes the following requirements:

- use of official (i.e. not personal) email addresses for user accounts;
- appropriate feedback and complaints information must be published in a prominent place which is easily accessible to other users;
- the school's logo and other branding elements should be used to indicate the school's support. The school's logo should not be used on social networking applications which are unrelated to or are not representative of the school's official position;
- users should identify themselves as their official position held within the school on social networking applications e.g. through providing additional information on user profiles;
- any contributions on any social networking application must be professional, uphold the reputation of the school and be in accordance with data protection requirements;
- users must not promote or comment on personal matters (including personal/ financial matters), commercial ventures, political matters or campaigns, religion or other matters;

Personal use of school Equipment/Networks

School equipment, internet services, systems and email may be used for incidental personal purposes, with the approval of the line manager, provided that it:

- does not interfere with the school's operation of computing facilities or email services;
- does not interfere with the user's employment or performance of professional duties or other obligations to the school;
- is of a reasonable duration and frequency;
- is carried out in authorised break times or outside their normal working hours;
- does not over burden the system or create any additional expense to the school;
- is not used to access, send, receive or store inappropriate material; and
- does not bring the school and its community into disrepute.

Workers must notify the school of any significant personal use.

Reasonable access and use of the internet/intranet and email facilities is available to recognised representatives of professional associations' i.e. union officers for the performance of their official duties and activities.

Email should be treated like any other form of written communication and, as such, the content should be appropriate and accurate and data protection compliant.

School equipment/networks/systems must additionally not be used for

- commercial purposes not under the auspices of the school;
- personal financial gain;
- personal use that is inconsistent of other school policies or guidelines; or
- ordering of goods to be delivered to the school address or in the school's name.

Use of personal ICT equipment in school

Mobile Phones

It is accepted that individuals may bring personal mobile phones to school. Personal mobiles should have security codes to prevent access by other persons and must be stored securely and not accessible to pupils at any time.

Workers are not permitted to use their personal mobile phones to call, text, email or in any other way message pupils. Nor may they divulge their personal telephone number(s) or other contact details to pupils under any circumstances.

Workers are required to ensure mobile telephones are switched off/to silent during working hours and accessed only during authorised breaks. Any urgent phone calls or messages must be directed to the office who will notify workers immediately. Workers who need to use their mobile telephone to make or receive an urgent call during working hours should where possible obtain prior authorisation from their line manager to do so.

There may be occasions where the use of a mobile phone is authorised, e.g. when one to one support workers may be working with pupils of high medical needs, or when staff take pupils to the bottom field (medical emergencies). Permission for this should be sought from the headteacher.

Other electronic devices

Workers should not bring other electronic devices onto school premises unless this has been specifically authorised by an appropriate manager. In such circumstances, the computer / equipment must be kept securely (at the risk of the owner) and security protected so that it cannot be accessed by pupils or others at the school.

Any personal use of such equipment must be restricted to an employee's break times or outside their normal working hours and must not impact on their duties in any way.

Additionally, specific permission must be obtained prior to connecting any device to school networks/systems and the device(s) must have adequate virus protection.

Workers must ensure that no personal information regarding school business, its pupils or staff is stored on such personal equipment.

Where exceptionally, specific permission is granted to use personal equipment for work purposes e.g. to give a presentation, the employee must be extremely vigilant that personal files/data etc. are not inadvertently accessed or displayed.

No pictures or videos may be taken within school or at any school related activity, on personal devices.

Personal social networks

The school recognises individual rights to privacy and a private life. However, the law generally views social media as in the public domain, irrespective of privacy settings. Workers are therefore advised to be mindful of their duties and obligations to uphold the reputation of the school, to comply with the Code of Conduct and other policies and contractual terms in their use of personal social media – being mindful of the real possibility for material to be posted, shared and made public inadvertently or by other contacts.

The school may require the removal of content it considers inappropriate.

It is totally unacceptable for any worker to discuss pupils, parents, work colleagues or any other member of the school community or any school related business on any type of social networking site.

Other posting on personal sites may also impact on the reputation of the school or the suitability/conduct of the employee for example if an employee is off sick but makes comments on a site to the contrary, postings of indecent or inappropriate images/activities etc.

Workers must not accept or propose contact, nor engage in any conversation with pupils on any personal social networking sites and should be circumspect in personal network contact with former pupils, particularly those under the age of 18 years.

Individuals working in the school should not use or access social networking sites of pupils.

Security

The school follows sound professional practices to secure data, system programmes, email records and networks under its control.

Workers must take all reasonable precautions to maintain security and confidentiality and to protect data. This includes:

- using appropriate security measures such as encryption/password protection to transmit

- confidential or sensitive information;
- ensuring all devices and system access are password protected using secured memory sticks (all laptops, memory sticks and devices used must be encrypted);
- ensuring that pupils are not exposed to any inappropriate images or web links; and
- respecting all copyrights and not copy, retrieve, modify or forward copyrighted materials except as permitted by the copyright owner.

Users must not:

- use, transfer or tamper with other people's accounts and files;
- use anonymous mailing services to conceal identity when mailing through the Internet, falsify e-mails to make them appear to originate from someone else, or provide false information to any Internet service which requests name, e-mail address or other details;
- use electronic media and services in a manner that is likely to cause network congestion or significantly hamper the ability of other people to access and use the system;
- store sensitive or confidential data on their own equipment – this extends to personal cameras, mobile phones and other similar devices;
- use the internet/intranet facilities or equipment to deliberately create any virus, worm, Trojan horse or any such other programme that is harmful to normal computer operations.
- monitor or intercept the files or electronic communications of other workers or third parties;
- hack or obtain access to systems or accounts they are not authorised to use;
- use other people's log-ins or passwords; or
- breach, test, or monitor computer or network security measures without authorisation.

Where any security breach or inappropriate connection or ICT activity occurs, the user must immediately disconnect/log out and report immediately.

Privacy and Monitoring

The school respects workers' privacy and will not routinely inspect or monitor emails, data or internet usage. However, workers should not have any expectation of absolute privacy in his or her use of the school systems or equipment (including but not limited to networks/servers/internet usage/networks/Wi-Fi). Under the following circumstances the school reserves the right, at its discretion, to review any electronic files and messages to the extent necessary to ensure systems are being used appropriately:

- when required by law;
- if there is a substantiated reason to believe that a breach of the law; or school's policy has taken place;
- if the school suspects that the employee has been viewing/transmitting offensive or illegal material;
- if the school suspects that the employee has been spending an excessive amount of time on activity which is not work related;

- where required for compliance checks eg auditors, data protection; or
- where there are emergency or compelling circumstances.

The school will endeavour to notify affected individuals of any monitoring which will take place and the reason for it, save in exceptional circumstances (see below).

Workers will normally be notified of what information will be recorded and retained, and for how long, who will have access and how such information will be used, which will include using such information for disciplinary purposes where applicable.

When monitoring emails, the school will, save in exceptional circumstances; confine itself to looking at the address and heading of the emails. Workers should mark any personal emails (where these are permitted by the school) as such and encourage those who send them to do the same. The school will avoid, where possible, opening emails clearly marked as private or personal.

The school considers the following to be valid reasons for checking an employee's email:

- if the employee is absent for any reason and communications must be checked for the smooth running of the school to continue;
- if the school suspects that the employee has been viewing or sending offensive or illegal material, such as material containing racist terminology or nudity (although the school understands that it is possible for workers inadvertently to receive such material and they will have the opportunity to explain if this is the case);
- if the school suspects that an employee has been using the email system to send and receive an excessive number of personal communications (or any personal emails if this is prohibited by the school); and
- if the school suspects that the employee is sending or receiving emails that are detrimental to the school or its pupils.

The school may monitor communications without notification in certain specific circumstances, including but not limited to;

- establish the existence of facts relevant to the school e.g. whether a contract was entered into by email;
- ascertain compliance with regulatory or self-regulatory practices e.g. checking that the school is complying with external or internal regulations;
- ascertain or demonstrate standards that are or ought to be achieved by workers using the system;
- investigate or detect unauthorised use of the telecommunication system, which would include checking that workers are not breaching the school's policy on email and internet use; and
- ensure the effective operation of the system, for example through virus monitoring.

Monitoring will be reasonable and in accordance with current legislation.

Covert monitoring

The use of covert monitoring will only be used in exceptional circumstances, for example, where the school suspects criminal activity or where telling the employee about the monitoring would make it difficult to prevent or detect such wrongdoing.

If the schools considers covert monitoring to be justified, this will only take place as part of a specific investigation, and will cease when the investigation has been completed.



Bentfield Primary School
Laptop Loan Agreement

The laptop and accessories remain the property of Bentfield Primary School and are only for the use of the member of staff to whom they have been issued. They must be returned when the member of staff ceases to be employed by the school. The laptop is issued to a member of staff for school related use and private use must be insignificant and incidental.

Under the school's insurance the laptop will be covered against theft and accidental damage provided the member of staff has taken reasonable precautions. Leaving an unattended laptop on view, either in a vehicle or around the school, would not be regarded as a reasonable precaution. Any theft must be reported to the police immediately and to the school as soon as possible.

If the laptop or any of the accessories are lost or damaged by a member of staff, s/he may be asked to contribute towards the cost of replacing them at the discretion of the Headteacher.

The school does not take responsibility for the loss of data files should a fault occur on the laptop. The member of staff to whom the laptop has been issued is responsible for ensuring that his/her data files are backed up on a regular basis.

Anti Virus and firewall software has been installed onto the laptop. The configuration settings must not be changed. The software must be kept regularly updated; it will automatically update when the laptop is connected to the Internet, but time must be allowed for the updates to finish. The period between consecutive updates should not exceed one week. If the laptop asks for a program to be granted access to the Internet, say "No" and check with the ICT Network Support Team.

Additional software may only be installed onto the laptop by the member of staff after s/he has provided the licence/proof of registration to the Strategic Leader of ICT Technologies who will note details for auditing purposes.

Any software found on the laptop that has not been approved by the ICT Network Support Team is subject to removal after a formal written notice has been issued.

Any telephone charges or fees payable to the Internet Service Provider incurred by the member of staff accessing the Internet from home are not chargeable to the school.

The laptop must be brought into school when requested so that software can be updated and annual electrical testing take place.

Equipment issued: Laptop, power cable, power adaptor, battery

Software loaded: Windows 10, MS Office, McAfee Security Centre (antivirus and firewall).

I have received the equipment and have read and understood the agreement.

Name

Signed

Date