Thomas A' Becket Infant School

Acceptable Use of ICT Policy

Introduction

At Thomas A' Becket Infant 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 others 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.

The school community has a shared responsibility to secure any sensitive information used in their day to day professional duties and all staff 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, regular visitors [for regulated activities] and pupils) include fixed and mobile internet; technologies provided by the school (such as PCs, laptops, mobile devices, 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 and other mobile devices).

Monitoring

Authorised ICT staff may inspect any ICT equipment owned or leased by the school at any time without prior notice.

All monitoring, surveillance or investigative activities are conducted by ICT authorised staff and comply with the UK General Data Protection Regulations (GDPR), the Human Rights Act 1998, Data Protection Act (amended) 2018, the Regulation of Investigatory Powers Act 2000 (RIPA) and the Lawful Business Practice Regulations 2000. Personal communications using School ICT may be included in any business communications that are monitored, intercepted and/or recorded.

Breaches

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

For staff, any policy breach is grounds for disciplinary action in accordance with the school Disciplinary Procedure.

Policy breaches may also lead to criminal or civil proceedings.

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

Incident Reporting

The following incidents should be reported to the school's relevant responsible person:

- Security breaches
- Lost/stolen equipment or data
- Unauthorised/misuse of ICT
- Virus notifications
- Policy non compliance

The relevant responsible individuals in the school are as follows: Head teacher, School Business Manager, and Computing Subject Leader. Please refer to the relevant section on Incident Reporting, eSafety Incident Log & Infringements.

THOMAS A'BECKET INFANT SCHOOL

The wording below is replicated in the Registration booklet completed by parents when each child starts school. Parents are asked for their consent (or not) and signature within the registration booklet.

As part of the school's ICT programme, we offer pupils supervised access to the wireless based internet. As you will appreciate from coverage on the media, it is very important for safeguards to be in place for the children to avoid misuse of the system.

Our Internet provider uses a fully filtered system, which safeguards children and prevents them from accessing unsuitable web sites. The filters cannot be changed or removed accidentally or without permission.

Access to the Internet has many advantages, giving children the opportunity to access libraries, databases, and to exchange messages with other educational establishments and appropriate contacts. However, families should be aware that some material on the Internet may contain items that are illegal, defamatory, inaccurate or potentially offensive. By using the filtered system, and exercising full supervision, the school will be making every effort to ensure that access to such material does not occur.

We believe that the benefits to children from access to the Internet in the form of information resources and opportunities for collaboration exceed any disadvantages.

We also have our own web site, and we have strict protocols about what this site can contain. We will not publish pupils' names or other personal information. From time to time we may put children's work on the web site but will ensure that it will only be accredited to a child by their first name. Our site is accessible on http://www.tabinfant.org.uk

May we reassure you that we will be most vigilant in monitoring your child's use of the Internet and access to websites. Before your child can use the Internet at school, we require parental permission. We need to ask parents and guardians of all pupils to consent (or not) to allow their children access to the internet (as detailed above) within the starting school registration booklet. Such consent can be withdrawn at any time by written request to the school or by e-mail to dpo@tabinfant.org.uk

I give / do not give my permission for my child to access school approved educational programmes such as Purple Mash / Espresso via the Internet. Basic Google searches may be undertaken to support learning topics (usually in Year 2). Such activities will take place using networked computers which have high level age relevant filtering in place.

I understand that my child will be fully supervised in the use of such services. I will not hold the school or the County Council responsible for inappropriate material which my child may obtain, and I accept responsibility for setting standards for my child to follow when selecting, sharing and exploring information and media.

Signature……Parent/Carer

Computer Viruses

- All files downloaded from the Internet, received via e-mail must be checked for any viruses using school provided anti-virus software before being used.
- Never interfere with any anti-virus software installed on school ICT equipment.
- If your machine is not routinely connected to the school network, you must make provision for regular virus updates with the ICT Technician.
- If you suspect there may be a virus on any school ICT equipment, stop using the equipment and contact your ICT Technician immediately. The ICT support provider will advise you what actions to take and be responsible for advising others that need to know.

Data Security

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

Security

- The school gives relevant staff access to the school network, SIMS and other systems, with a unique username and password
- It is the responsibility of everyone to keep passwords secure. Temporary passwords must be changed on initial log in. All passwords must be 'strong' and contain at least 8 characters including upper case / lower case, numbers and symbols. *(it is currently recommended that to minimize the risk of passwords being hacked, they should be a minimum of 13 characters including random words and numbers)*
- Staff are aware of their responsibility when accessing school data
- Staff have been issued with the relevant guidance documents and the Policy for ICT Acceptable Use
- Leadership have identified relevant responsible persons
- Staff keep all school related data secure. This includes all personal, sensitive, confidential or classified data
- Removable media devices such as memory sticks are not to be used.
- Staff must avoid leaving any portable or mobile ICT equipment in unattended vehicles. Where this is not possible, keep it locked out of sight
- Staff should always carry portable and mobile ICT equipment 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, confidential and classified information contained in documents faxed, copied, scanned or printed. This is particularly important when shared copiers (multi-function print, fax, scan and copiers) are used

Protective Marking

- Appropriate labelling of data should help schools secure data and so reduce the risk of security incidents
- Applying too high a protective marking can inhibit access, lead to unnecessary and expensive protective controls, and impair the efficiency of an organisation's business
- Applying too low a protective marking may lead to damaging consequences and compromise of the asset
- The sensitivity of an asset may change over time and it may be necessary to reclassify assets. If a document is being de-classified or the marking changed, the file should also be changed to reflect the highest marking within its contents

- 3 levels of labelling are recommended
    - Unclassified (or if unmarked) – this will imply that the document contains no sensitive or personal information and will be a public document
    - Protect – this should be the default setting and be applied to documents containing any sensitive or personal data. Marking documents as Protect will demonstrate an awareness of the Data Protection Act and the school's responsibilities
    - Restricted – documents containing any ultra-sensitive data for even one person should be marked as Restricted

Relevant Responsible Persons

Senior members of staff should be familiar with information risks and the school's response:

- They lead on the information risk policy and risk assessment
- They advise school staff on appropriate use of school technology
- They act as an advocate for information risk management

Information Asset Owner (IAO)

Any information that is sensitive needs to be protected. This will include the personal data of learners and staff; such as assessment records, medical information and special educational needs data. The Data Protection Officer (DPO) should be able to identify across the school:

- What information is held, and for what purposes (held on data mapping spreadsheet)
- What information needs to be protected 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

As a result the DPO is able to manage and address risks to the information and make sure that information handling complies with legal requirements.

However, it should be clear to all staff that the handling of secured data is everyone's responsibility – whether they are an employee, consultant, software provider or managed service provider. Failing to apply appropriate controls to secure data could amount to gross misconduct or even legal action.

Disposal of Redundant ICT Equipment Policy

- All redundant ICT equipment will be disposed of through an authorised agency. This should include a written receipt for the item including an acceptance of responsibility for the destruction of any personal data
- All redundant ICT equipment that may have held personal data will have the storage media over written multiple times to ensure the data is irretrievably destroyed. Or if the storage media has failed it will be physically destroyed. We will only use authorised companies who will supply a written guarantee that this will happen
- Disposal of any ICT equipment will conform to:
- The Waste Electrical and Electronic Equipment Regulations 2006
- The Waste Electrical and Electronic Equipment (Amendment) Regulations 2007

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

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

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

Data Protection Act 1998

https://ico.org.uk/for-organisations/education/

Electricity at Work Regulations 1989

http://www.opsi.gov.uk/si/si1989/Uksi_19890635_en_1.htm

- The school will maintain a comprehensive inventory of all its ICT equipment including a record of disposal
- The school's disposal record will include:
    - Date item disposed of
    - Authorisation for disposal, including:
        - verification of software licensing
        - any personal data likely to be held on the storage media? *

- How it was disposed of e.g. waste, gift, sale
- Name of person & / or organisation who received the disposed item

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

Waste Electrical and Electronic Equipment (WEEE) Regulations

Environment Agency web site

Introduction

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

The Waste Electrical and Electronic Equipment Regulations 2006

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

The Waste Electrical and Electronic Equipment (Amendment) Regulations 2007

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

Information Commissioner website

https://ico.org.uk/

Guide to the General Data Protection Regulation (GDPR) | ICO

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

PC Disposal – SITSS Information

http://www.thegrid.org.uk/info/traded/sitss/services/computer_management/pc_disposal

E-mail

In the context of school, e-mail should not be considered private.

Managing e-mail

- The school gives all staff and governors their own e-mail account to use for all school business as a work based tool This is to protect staff, 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, parents or conduct any school business using personal e-mail addresses

- School e-mails must not be forwarded / auto-forwarded to personal e-mail accounts of staff / governors. However you access your school e-mail (whether directly, through webmail when away from the office or on non-school hardware), e-mails must only be accessed from a secure and lockable device.

- 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 or parents are advised to cc. the Head teacher where appropriate

- E-mails created or received as part of an individual's role will be subject to disclosure in response to a request for information under the Freedom of Information Act 2000. Staff 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

- Staff must inform (the Head teacher) if they receive an offensive e-mail

- The Acceptable use of IT and Data Protection policies apply at all times

- Sending e-mails - 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

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

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

Receiving e-mails

- Check your e-mail regularly

- Activate your 'out-of-office' notification when away for extended periods

- Never open attachments from an untrusted source; Consult the ICT Technician first

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

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

E-mailing Personal, Sensitive, Confidential or Classified Information

- Where e-mail must be used to transmit such data:

  - Exercise caution when sending the e-mail and always follow these checks before releasing the e-mail:

    - Encrypt and / or password protect.
    - 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
    - Anonymise names of individuals within e-mails (particularly within the e-mail subject field) – i.e. use initials rather than names
    - Do not copy or forward the e-mail to any more recipients than is absolutely necessary

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

Equal Opportunities

Access to the school's ICT facilities is available to all members of the school community in accordance with the school's Equal Opportunities Policy.

ESafety

eSafety - Roles and Responsibilities

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 eSafety co-ordinator in this school is *the Head teacher.* All members of the school community have been made aware of who holds this post. It is the role of the eSafety co-ordinator to keep abreast of current issues and guidance through organisations such as CEOP (Child Exploitation and Online Protection) and Childnet.

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

This policy, supported by the school's acceptable use agreements for staff, governors, visitors and 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 PSHCE.

eSafety in the Curriculum

eSafety guidance is given to 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 internet skills in Computing lessons
- The school provides opportunities within a range of curriculum areas to teach eSafety
- Educating pupils about the online risks that they may encounter outside school is done informally when opportunities arise and as part of the eSafety curriculum
- Pupils are taught to critically evaluate materials and learn good researching skills through cross curricular teacher models, discussions and via the Computing curriculum
- The key eSafety advice will be promoted through the school's website

eSafety Skills Development for Staff

- All staff are aware of their individual responsibilities relating to the safeguarding of children within the context of eSafety and know what to do in the event of misuse of technology by any member of the school

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

Incident Reporting, eSafety Incident Log & Infringements

Incident Reporting

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

eSafety Incident Log

An e-safety incident will be logged with the Head teacher who will take necessary action.

Misuse and Infringements

Complaints

Complaints and/ or issues relating to eSafety should be made to the eSafety co-ordinator/Head teacher. Incidents should be logged and the relevant procedures should be followed.

Inappropriate Material

- All users are aware of the procedures for reporting accidental access to inappropriate materials. The breach must be immediately reported to the eSafety co-ordinator
- Deliberate access to inappropriate materials by any user will lead to the incident being logged by the relevant responsible person, and an investigation by the Head teacher. Depending on the seriousness of the offence, sanctions could include immediate suspension, possibly leading to dismissal and involvement of police for very serious offences

Internet Access

Managing the Internet

- The school provides pupils with supervised access to Internet resources (where reasonable) through the school's fixed and mobile internet connectivity
- Staff will preview any recommended sites, online services, software and apps before use
- Searching for images through open search engines is discouraged when

working with pupils

- 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

- Personal, sensitive, confidential or classified information or the dissemination of such information that may compromise the intended restricted audience must not be posted

- Names of colleagues, pupils, others or any other confidential information acquired must not be revealed on any social networking site or other online application

- On-line gambling or gaming is not allowed

It is at the Head teacher's discretion which internet activities are permissible for staff and pupils and how this is disseminated.

Infrastructure

- School internet access is controlled through a web filtering service.

- Thomas A' Becket Infant School is aware of its responsibility when monitoring staff communication under current legislation and takes into account; UK General Data Protection Regulation (GDPR), Data Protection Act (amended) 2018 The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, Regulation of Investigatory Powers Act 2000, Human Rights Act 1998

- Staff 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

- The school uses management control tools for controlling and monitoring workstations

- If staff or pupils discover an unsuitable site, the screen must be switched off/ closed and the incident reported immediately to the e-safety coordinator or teacher as appropriate

- It is the responsibility of the school, by delegation to the network manager, to ensure that anti-virus protection is installed and kept up-to-date on all school machines

- Pupils and staff are not permitted to download programs or files on school based technologies without seeking prior permission from the Head teacher/technician.

- If there are any issues related to viruses or anti-virus software, the network manager should be informed by logging this in the communication folder.

Managing Other Online Technologies

At present, the school endeavours to deny access to social networking and online games websites to pupils within school

- Services which some children seem to access outside of school, such as Facebook and Instagram have a 13+ age rating which should not be ignored http://www.coppa.org/comply.htm

Parental Involvement

Parents/carers should be fully involved with promoting eSafety both in and outside of school and 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 of new technologies, together with the associated risks.

- Parents/carers are asked to read through and sign an Internet Access consent on behalf of their child on admission to the school
- Parents/carers are required to make a decision as to whether they consent to images of their child being taken and used in the public domain (e.g., on school website)
- Parents/carers are expected to sign a Home School agreement
- The school disseminates information to parents relating to eSafety where appropriate in the form of;
    - Information evenings
    - School website information
    - Newsletter items

Passwords and Password Security

Passwords

- **Always use your own** personal passwords
- Make sure you enter your personal passwords each time you logon. Do not include passwords in any automated logon procedures
- Staff should change temporary passwords at first logon
- Change passwords whenever there is any indication of possible system or password compromise
- Do not record passwords or encryption keys on paper or in an unprotected file
- **Only disclose your personal password to authorised ICT support staff when necessary, and never to anyone else**. Ensure that all personal passwords that have been disclosed are changed once the requirement is finished
- **Never tell a child or colleague your password**
- **If you aware of a breach of security with your password or account (i.e. someone else has become aware of your password) inform the DPO immediately**
- Passwords must contain a minimum of eight characters, including upper and lower case letters, numbers and symbols and be difficult to guess. *(it is currently recommended that to minimize the risk of passwords being hacked, they should be a minimum of 13 characters including random words and numbers)*

Password Security

- All users read and sign an Acceptable Use Agreement to demonstrate that they have understood the school's e-Safety Policy and Data Security
- Users are provided with an individual network, email, Insight and Bromcom log-in username.
- Pupils are not allowed to deliberately access on-line materials or files on the school network or local storage devices of their peers, teachers or others
- Staff are aware of their individual responsibilities to protect the security and confidentiality of the school networks and systems 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.
- All staff are expected to comply with ICT password policies at all times

Zombie Accounts

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

- Ensure that all user accounts are disabled once the member of the school has left. Prompt action on disabling accounts will prevent unauthorized access
- Regularly change generic passwords to avoid unauthorised access (Microsoft® advise every 42 days)

Personal or Sensitive Information

Protecting Personal, Sensitive, Confidential and Classified Information

- Ensure that any school information accessed from your own PC is kept secure. School information / data must not be saved to laptops or removable storage devices (e.g. memory sticks). Ensure you lock your screen before moving away from your computer during your normal working day to prevent unauthorised access
- Ensure the accuracy of any personal, sensitive, confidential and classified information you disclose or share with others
- Ensure that personal, sensitive, confidential or classified information is not disclosed to any unauthorised person
- Ensure the security of any personal, sensitive, confidential and classified information contained in documents you fax, copy, scan or print. This is particularly important when shared copiers (multi-function print, fax, scan and copiers) are used and when access is from a non-school environment
- Only download personal data from systems if expressly authorised to do so
- You must not post on the internet personal, sensitive, confidential, or classified information, or disseminate such information in any way that may compromise its intended restricted audience
- Keep your screen display out of direct view of any third parties when you are accessing personal, sensitive, confidential or classified information
- Ensure hard copies of data are securely stored and disposed of after use in accordance with the document labeling

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

- Removable media e.g. memory sticks are not to be used
- Store all removable media (e.g. laptops / iPads) securely at all times. Information must not be saved to laptops.
- Securely dispose of removable media that may hold personal data

- Password protect all files containing personal, sensitive, confidential or classified data

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

Remote Access

- You are responsible for all activity via your remote access facility

- Only use equipment with an appropriate level of security for remote access (including accessing work e-mails)

- To prevent unauthorised access to school systems, keep all access information such as IP addresses telephone numbers, logon IDs and PINs confidential and do not disclose them to anyone

- Select PINs to ensure that they are not easily guessed, e.g. do not use your house or telephone number or choose consecutive or repeated numbers

- Avoid writing down or otherwise recording any network access information. Any such information that is written down must be kept in a secure place and disguised so that no other person will be able to identify what it is

- Protect school information and data at all times, including any printed material produced while using the remote access facility. Take particular care when access is from a non-school environment

- When logged on remotely from home to the school server, lock the home PC screen whenever you leave the workstation

- School information / data must not be saved to home computers

Safe Use of Images

Taking of Images and Film

- 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 permitted to use personal digital equipment, such as mobile phones and cameras, to record images of pupils, this includes when on trips.

- Pupils are not permitted to use personal digital equipment, including mobile phones and cameras, to record images of pupils, staff and others

- Pupils and staff must have permission from the Head teacher before any image can be uploaded for publication

Publishing Pupil's Images and Work

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

- on the school web site
- in the school prospectus and other printed publications that the school may produce for promotional purposes
- recorded/ transmitted on a video or webcam
- in display material that may be used in the school's communal areas
- in display material that may be used in external areas, 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)

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

Parents or carers may withdraw permission, in writing, at any time. Consent must also be given in writing and will be kept on record by the school.

Pupils' names will not be published alongside their image and vice versa. Pupils' full names will not be published.

Only the Senior Leadership Team and SEN Administrator have authority to upload to the internet.

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)
- Rights of access to this material are restricted to the teaching staff and pupils within the confines of the school network or other online school resource
- All staff who have saved images have the responsibility of deleting the images when they are no longer required, or when the pupil has left the school

Webcams and CCTV

- We do not use publicly accessible webcams in school
- Webcams will not be used for broadcast on the internet
- CCTV images are retained on the system until memory storage is full, and then overwritten in chronological order. The system usually retains between ten and fourteen days most recent school days recordings.

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

School ICT Equipment

- As a user of the school ICT equipment, you are responsible for your activity
- ICT equipment issued to staff is logged and serial numbers are recorded as part of the school's inventory
- Do not allow your visitors to plug their ICT hardware into the school network points (unless special provision has been made). They should be directed to the wireless ICT facilities if available
- Ensure that all ICT equipment that you use is kept physically secure
- Do not attempt unauthorised access or make unauthorised modifications to computer equipment, programs, files or data. This is an offence under the Computer Misuse Act 1990
- It is imperative school data is only saved to and accessed from the school's network. Personal or sensitive data must not be stored on the local drives of desktop PC, laptop, USB memory stick or other portable device.
- It is recommended that a time locking screensaver is applied to all machines. Any device accessing personal data must have a locking screensaver as must any user profiles
- Privately owned ICT equipment should not be used on a school network
- On termination of employment, resignation or transfer, return all ICT equipment. You must also provide details of all your system logons so that they can be disabled
- It is your responsibility to ensure that any information accessed from your own PC or school laptop is kept secure, and that no personal, sensitive, confidential or classified information is disclosed to any unauthorised person
- All ICT equipment allocated to staff must be authorised by the appropriate Line Manager. The ICT Co-ordinator is responsible for:

- maintaining control of the allocation
- recovering and returning equipment when no longer needed

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

Portable & Mobile ICT Equipment

This section covers such items as laptops, iPads, and mobile devices. Please refer to the relevant sections of this document when considering storing or transferring personal or sensitive data. Removable storage devices must not be used.

- 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 the school network, and not kept on the laptop. 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 / iPad in the boot of your car before starting your journey

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

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

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

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

Mobile Technologies

Personal Mobile Devices (including phones)

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

- Pupils are not allowed to bring personal mobile devices/phones to school

- 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

School Provided Mobile Devices (including phones)

- Where the school provides mobile technologies such as phones, laptops and iPads for offsite visits and trips, only these devices should be used
- Where the school provides a laptop for staff, only this device may be used to conduct school business outside of school

Servers

- Always keep servers in a locked and secure environment
- Limit access rights
- Always password protect and lock the server
- Existing servers should have security software installed appropriate to the machine's specification
- Data must be backed up regularly. The school backs up data daily via Capita Redstor, a secure encrypted cloud based system.
- Back up media stored off-site must be secure
- Remote backups should be automatically securely encrypted.

Social Media, including Facebook and Twitter

- Staff ***are not*** permitted to access their personal social media accounts using school equipment
- Pupils are not permitted to access any personal game/media accounts whilst at school
- Staff, governors, parents and carers are regularly provided with information on how to use social media responsibly and what to do if they are aware of inappropriate use by others
- Staff, governors, parents and carers are aware that the information, comments, images and video they post online can be viewed by others, copied and stay online forever
- Staff, governors, parents and carers are aware that their online behaviour should at all times be compatible with UK law

Systems and Access

- You are responsible for all activity on school systems carried out under any access/account rights assigned to you, whether accessed via school ICT equipment or your own PC
- Do not allow any unauthorised person to use school ICT facilities and services that have been provided to you
- Use only your own personal logons, account IDs and passwords and do not allow them to be used by anyone else
- Keep your screen display out of direct view of any third parties when you are accessing personal, sensitive, confidential or classified information
- Ensure you lock your screen before moving away from your computer during your normal working day to protect any personal, sensitive, confidential or otherwise classified data and to prevent unauthorised access
- Ensure that you logoff from the PC completely when you are going to be away from the computer for a longer period of time. PCs must be shut down at the end of each day.
- Do not introduce or propagate viruses
- It is imperative that you do not access, load, store, post or send from school ICT any material that is, or may be considered to be, illegal, offensive, libelous, pornographic, obscene, defamatory, intimidating, misleading or disruptive to the school or may bring the school into disrepute. This includes, but is not limited to, jokes, chain letters, files, emails, clips or images that are not part of the school's business activities; sexual

comments or images, nudity, racial slurs, gender specific comments, or anything that would offend someone on the basis of their age, sexual orientation, religious or political beliefs, national origin, or disability (in accordance with the Sex Discrimination Act, the Race Relations Act and the Disability Discrimination Act)

- Any information held on School systems, hardware or used in relation to School business may be subject to The Freedom of Information Act
- Where necessary, obtain permission from the owner or owning authority and pay any relevant fees before using, copying or distributing any material that is protected under the Copyright, Designs and Patents Act 1998
- It is essential that any hard drives which may have held personal or confidential data are 'scrubbed' in way that means the data can no longer be read. It is not sufficient to simply delete the files or reformat the hard drive. Whoever you appoint to dispose of the equipment must provide a **written guarantee** that they will irretrievably destroy the data by multiple over writing the data.

Telephone Services

- You may make or receive personal telephone calls provided:

    1. They are infrequent, kept as brief as possible and do not cause annoyance to others
    2. They are not for profit or to premium rate services
    3. They conform to this and other relevant school policies.

- School telephones are provided specifically for school business purposes and personal usage is a privilege that will be withdrawn if abused
- Be aware that the laws of slander apply to telephone calls. Whilst a telephone call may seem to have a temporary and private existence it still qualifies as admissible evidence in slander law cases
- Ensure that your incoming telephone calls can be handled at all times
- Follow the appropriate procedures in the event of receiving a telephone call containing a bomb threat. These procedures should be made readily available throughout your office.

Writing and Reviewing this Policy

Staff Involvement in Policy Creation

- Staff and governors and have been involved in making/ reviewing the Policy for ICT Acceptable Use through meetings.

Review Procedure

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

There will be on-going opportunities for staff to discuss with the Headteacher / Data Protection Officer any issue of data security that concerns them

This policy will be reviewed every 12 months and consideration given to the implications for future whole school development planning

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

This policy was originally approved by Governors on 22nd May 2018 and updated annually since. Any changes by WSCC to this policy / procedures will be reviewed as and when we are notified.

Current Legislation

Acts Relating to Monitoring of Staff email

General Data Protection Regulations (GDPR)

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.

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 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.

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

Public Order Act 1986 (sections 17 – 29)

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

Protection of Children Act 1978 (Section 1)

It is an offence to take, permit to be taken, make, possess, show, distribute or advertise indecent images of children in the United Kingdom. A child for these purposes is 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

General Data Protection Regulation

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

The Freedom of Information Act 200

https://ico.org.uk/for-organisations/guide-to-freedom-of-information/

Committee	Signed by:	Date
Leadership & Management	**Chair – Ruth Hilliard**	**24 May 2022**

Review Date	Summer 2023 or as guidance changes