E-Safety Policy

Date Policy Updated:	February, 2025
Leadership team responsibility To Present to A&P Committee	Gbenga Sonuga, Deputy Headteacher February 2025
Date Policy Ratified:	May, 2025
Date for next Review:	February, 2026

Contents

Introduction

This policy is designed to provide a full overview of all aspects of E-Safety within the school and to provide a fully comprehensive insight into the protocols and procedures that are followed. It should be read in conjunction with the school's Online Safety Policy and Data Protection Policy.

At Bishop Stopford's School**,** we understand the responsibility to educate our pupils and our staff on e-Safety 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. The provisions outlined in this policy work in tandem with the provisions outlined in the school's behaviour and data protection policies.
As is standard, the school holds personal data on learners, staff and others to help them conduct their day-to-day activities. Everybody in the school community has a shared responsibility to secure any sensitive information used in their day-to-day professional duties and even staff not directly involved in data handling are made aware of the risks and threats and how to minimise them. For more details of the school's policies and protocols regarding data protection, see the school's **data protection policy**.

E-Safety - Roles and Responsibilities

As e-Safety is an important aspect of strategic leadership within the school, the Headteacher and governors have ultimate responsibility to ensure that the policy and practices are embedded and monitored. The named e-Safety co-ordinator in this school is Mr Blake, the Designated Senior Person is Mr Sonuga. All members of the school community have been made aware of who holds this post. It is the role of the e-Safety co-ordinator to keep abreast of current issues and guidance through organisations such as Enfield LA, Enfield Council HUB, CEOP (Child Exploitation and Online Protection) and Childnet.

Senior Leadership Team and governors are updated by the e-Safety co-ordinator through the work of governor's monitoring groups and all governors understand the issues and strategies at our school in relation to local and national guidelines.

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 PSHE programme and the following mandatory school policies and key documents: **Child Protection Policy**, **Health and Safety policy**, **Behaviour and Discipline policy and Anti-bullying policy**.

Monitoring of E-Safety

Authorised ICT staff may inspect any ICT equipment owned or leased by the school at any time without prior notice. If you are in doubt as to whether the individual requesting such access is authorised to do so, please contact the Designated Senior Person or Headteacher.
ICT authorised staff and service providers may monitor, intercept, access, inspect, record and disclose telephone calls, e-mails, instant messaging, internet/intranet use and any other electronic communications (data, voice, video or image) involving its employees or contractors, without consent, to the extent permitted by law. 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 1998, or to prevent or detect crime.
ICT authorised staff may, without prior notice, access the e-mail or voice-mail account where applicable, of someone who is absent in order to deal with any business-related issues retained on that account, with the approval of the Deputy Headteacher or Headteacher.

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

Breaches of this policy

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, disciplinary procedures will be followed in line with school's behaviour policy.

Reporting of breaches

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 relevant responsible person. Additionally, all security breaches, lost/stolen equipment or data (including remote access SecureID tokens and PINs), virus notifications, unsolicited emails, misuse or unauthorised use of ICT and all other policy non-compliance must be reported to the relevant responsible person. The relevant responsible individuals in the school are: Designated Senior Person and e-Safety co-ordinator.

Computer Viruses

- All files downloaded from the Internet, received via e-mail or on removable media such as a memory stick 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 the machine a member of staff is using is not routinely connected to the school network, you must make provision for regular virus updates through the Network team.

If you suspect there may be a virus on any school ICT equipment, stop using the equipment and contact network staff immediately. Network staff will advise you what actions to take and be responsible for advising others that need to know.

E-Safety in the Curriculum

ICT and online resources are increasingly used across the curriculum. We believe it is essential for e-Safety guidance to be given to the pupils on a regular and meaningful basis. E-Safety is embedded within our curriculum and we continually look for new opportunities to promote e-Safety.
The school provides opportunities within a range of curriculum areas to teach about e-Safety through KS3 Computer Science lessons, assemblies, and through the PSHCE programme

- Educating pupils about the online risks that they may encounter outside school is done informally when opportunities arise and as part of the e-Safety curriculum
- Pupils are aware of the relevant legislation when using the internet such as data protection and intellectual property which may limit what they want to do but also serves to protect them

- Pupils are taught about copyright, respecting other people's information, safe use of images and video and other important areas through discussion, modelling and appropriate activities
- Pupils are aware of the impact of Cyberbullying and know how to seek help if they are affected by any form of online bullying. Pupils are also aware of where to seek advice or help if they experience problems when using the internet and related technologies; e.g. Heads of Year, Form Tutors, organisations such as CEOP and Childnet
- Pupils are taught to critically evaluate materials and learn good searching skills through the computing curriculum
- The school will ensure that the role of e-safety in preventing radicalisation is incorporated into the PSHE programme (see the more detailed outline of the school's commitment to the Prevent agenda as outlined in the Child Protection Policy)

E-Safety - Skills Development for Staff

- Our staff receive regular information and training on e-Safety and how they can promote the 'Stay Safe' online messages in the form of staff briefings and staff meetings
- New staff receive information on the school's acceptable use policy as part of their induction
- All staff have been made aware of their 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 and ensure they are adequately informed with up-to-date areas of concern.
- A statement of key professional responsibilities for staff with respect to e-Safety, approved by representatives of professional bodies including trade unions is included as an appendix to this policy (see Appendix 4)

Managing the School e-Safety Messages

- We endeavour to embed e-Safety messages across the curriculum whenever the internet and/or related technologies are used
- The key e-Safety advice will be promoted widely through school displays, newsletters, class activities and assemblies

Incident Reporting, e-Safety Incident Log & Infringements

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

Complaints

Complaints and/or issues relating to e-Safety should be made to the e-Safety co-ordinator or Headteacher. Incidents should be logged.

Inappropriate Material

- All users are aware of the procedures for reporting accidental access to inappropriate materials. The breach must be immediately reported to the e-Safety 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 Headteacher or Deputy Headteacher. Depending on the seriousness of the offence, sanctions could include immediate suspension, possibly leading to dismissal and involvement of police for very serious offences.
- Users are made aware of sanctions relating to the misuse or misconduct by the staff handbook

Internet Access

The internet is an open worldwide communication medium, available to everyone, 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 internet use through the school's network is logged and the logs are regularly monitored. Whenever any inappropriate use is detected, it will be followed up. Web filtering is managed via the Impero system, Smoothwall and LGFL used by many schools nationally and fully compliant with KCSIE 2024.

If a concern regarding Prevent is detected externally, the Headteacher, e-Safety coordinator and Senior Designated Person receive Prevent Alerts from the Enfield Prevent Team or other relevant external agencies. An e-mail will be sent automatically from enfieldprevent.org to them if any school internet sessions are detected with an attempt to access extremist material on the internet.

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 preview any recommended sites, online services, software and apps before use
- If Internet research is set for homework, specific sites will be suggested that have previously been checked by the teacher. Parents are advised to supervise any further research
- All users must observe software copyright at all times. It is illegal to copy or distribute school software or illegal software from other sources
- All users must observe copyright of materials from electronic resources

Internet Use by staff

- All staff are advised not to post personal, sensitive, confidential or classified information or disseminate such information in any way that may compromise themselves or their intended audience
- Staff are advised to not reveal names of colleagues, pupils, others or any other confidential information acquired through their job on any social networking site or other online application

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

Infrastructure

- LGFL manage the school's internet connection through RM Education which is filtered and monitored by the Smoothwall and Impero systems.

- School internet access is controlled through the LGFL web filtering service. For further information relating to filtering please go to
  https://www.enfield.gov.uk/safeguardingenfield/support-for-parents-and-carers/keeping-your-child-safe-online
- Bishop Stopford's School is aware of its responsibility when monitoring staff communication under current legislation and takes into account; Data Protection Act 1998, The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations

2000, Regulation of Investigatory Powers Act 2000, Human Rights Act 1998

- Staff and pupils are aware that school-based email and internet activity can be monitored and explored further if required
- The school does not allow pupils access to internet logs
- 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, network staff or teacher as appropriate, ideally via the ICT Helpdesk
- It is the responsibility of the school, by delegation to the network staff, to ensure that anti-virus protection is installed and kept up-to-date on all school devices
- Pupils and staff are not encouraged to use portable, removable media. Where used devices should be encrypted for security and only be used for specific tasks. Many of the traditional uses of removable storage have been replaced with cloud storage such as Google Drive
- 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 neither the school nor network staff's responsibility to install or maintain virus protection on personal systems.
- If pupils wish to bring in work on removable media it must be given to the network team for a safety check first
- Pupils and staff are not permitted to download programs or files on school-based technologies without seeking prior permission from the network staff
- If there are any issues related to viruses or anti-virus software, the network team should be informed. Students cannot delete their internet history.

Managing Other Online Technologies

Online technologies, including social networking sites, if used responsibly both outside and within an educational context can provide easy to use, creative, collaborative and free facilities. However, it is important to recognise that there are issues regarding the appropriateness of some content, contact, culture and commercialism. To this end, we encourage our pupils to think carefully about the way that information can be added and removed by all users, including themselves, from these sites.

- At present, the school endeavours to deny access to social networking and online games websites to pupils within school
- All pupils are advised to be cautious about the information given by others on such websites, for example users not being who they say they are
- Pupils are taught to avoid placing images or video of themselves (or details within images or video that could give background details) on such websites and to consider the appropriateness of any images or video they post due to the difficulty of removing an image or video clip once online
- Pupils are always reminded to avoid giving out personal details on websites which may identify them or where they are (full name, address, mobile/ home phone numbers, school details, IM/ email address, specific hobbies/ interests)
- Pupils are advised to set and maintain their online profiles to maximum privacy and deny access to unknown individuals
- Pupils are encouraged to be wary about publishing specific and detailed private thoughts and information online
- Pupils are asked to report any incidents of cyberbullying to the Head of Year.
- Staff should only communicate with pupils through Google Workspace Apps including Google Classroom and email. If staff wish to create external blogs, wikis or other online areas in order to communicate with pupils they must be approved by the Headteacher
- Services such as Facebook and Instagram have a 13+ age rating which should not be ignored, compliance with age guidelines is encouraged in the school's e-Safety guide for parents

Parental Involvement

We believe that it is essential for parents/carers to be fully involved with promoting e-Safety both in and outside of school and to be aware of their responsibilities. We regularly consult and discuss e-Safety with parents/ carers and seek to promote a wide understanding of the benefits of new technologies, together with the associated risks.

- Parents/carers and pupils are actively encouraged to contribute to adjustments or reviews of the school e-Safety policy through parent information evenings and by the school's e Safety guide
- Parents/carers are asked to read through and sign the Home School Agreement with their child on admission to the school (see appendix 1)
- Parents/carers are required to make a decision as to whether they consent to images or video of their child being taken and 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;
    - School website information
    - Newsletter items
    - Emails with updates to policies or procedures

Passwords and Password Security

Staff and students are asked to read and agree to the school's acceptable usage policy (see appendices 1 and 2) annually.

Visitor and governor access to the school network, in the rare occasions when this is authorised by the Deputy Headteacher, will also be subject to the acceptable use agreement (appendix 3). For sensitive documents that are transferred electronically staff should use the Egress system https://reader.egress.com/?_gl=1*1mt8ocm*_gcl_au*MjA2ODI4MjI5OS4xNzI5Njc2ODk4&rtkt=607f0adf-1db2530e4b32db0

Staff are encouraged to use the following guidelines when using 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 inform network staff immediately**
- Passwords must contain a minimum of eight characters and be difficult to guess
- Passwords should contain a mixture of upper and lowercase letters, numbers and symbols. Good passwords consist of 3 or 4 words, joined by numbers or symbols
- Access to password protected areas of the network or external sites is removed when a member of staff leaves

Safe Use of Images and Video

Digital images and video are easy to capture, reproduce and publish and, therefore, misuse. We must remember that it is not always appropriate to take or store images or video of any member of the school community or public, without first seeking consent and considering the appropriateness.

- With the written consent of parents (on behalf of pupils) and staff, the school permits the appropriate taking of images or video 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 or video of pupils, this includes when on field trips. However, with the express permission of the Headteacher, images or video can be taken provided they are transferred immediately and solely to the school's network and deleted from the staff device
- Pupils are not permitted to use personal digital equipment, including mobile phones and cameras, to record images or video of pupils, staff and others
- Pupils and staff must have permission from the Headteacher before any image or video can be uploaded for publication

Publishing Pupil's Images, Video and Work

On a child's entry to the school, all parents/carers will be asked to give consent to use their child's work, photos or video 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
- on the school's learning platform or Google Workspace
- 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
- social media posts (such as Facebook / Instagram)
- 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 consent, in writing, at any time. Consent must also be given in writing and will be kept on record by the school.

Pupils' full names will not be published alongside their image and vice versa. E-mail and postal addresses of pupils will not be published. Pupils' full names will never be published.
Before posting student work on the Internet, a check needs to be made to ensure that consent has been given for work to be displayed.

For further information relating to issues associated with school websites and the safe use of images in Hertfordshire schools, see:

Storage of Images

- Images or videos of children are stored on the school's network
- Pupils and staff are not permitted to use personal portable media for storage of images or video (e.g., USB sticks) without the express permission of the Headteacher
- Rights of access to this material are restricted to the teaching staff and pupils within the confines of the school network or other online school resource

Webcams and CCTV

- The school uses CCTV for security and safety. Notification of CCTV use is displayed at the front of the school. Please refer to the hyperlink below for further guidance
  CCTV Policy for viewing
- The school does not use publicly accessible webcams
- Webcams will not be used for broadcast on the internet without prior parental consent
- Misuse of the webcam by any member of the school community will result in sanctions (as indicated in the 'inappropriate materials' section of this document)
- Consent is sought from parents/carers and staff on joining the school, in the same way as for all images
- Webcams include any camera on an electronic device which is capable of producing video (e.g. tablet devices). School policy should be followed regarding the use of such personal devices

Google Meet, Microsoft Teams & Zoom

- Google Meet, Microsoft Teams and Zoom are the platforms regularly used for remote teaching between a classroom and teachers
- School Cloud may be used for Parent Evening consultations

School ICT Equipment including Chromebooks (whether leased or owned), Portable & Mobile ICT Equipment & Removable Media

- As a user of school ICT equipment, staff are responsible for their own activity
- The school maintains a log of ICT equipment issued to staff and records serial numbers as part of the school's inventory
- Visitors are not allowed 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
- The school ensures that as far as possible ICT equipment is kept physically secure e.g. locked server room and the physical locking down of classroom-based PCs
- Staff are not allowed 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 that staff save their data on a frequent basis to the school's network. Staff are responsible for the backup and restoration of any of their data that is not held on the school's network
- Personal or confidential data should not be stored on the local drives of desktop PC, laptop, USB memory stick or any other portable device. If it is necessary to do so the local drive must be encrypted
- 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 devices or equipment should not be used on a school network, unless permission is obtained from network staff
- On termination of employment, resignation or transfer, return all ICT equipment to your Manager. Departing staff must also provide details of all their system logons so that they can be disabled
- Personal, sensitive, confidential or classified information relating to students should not be stored on your personal equipment or portable media. All ICT equipment allocated to staff must be authorised by the appropriate Line Manager. Authorising Managers are responsible for:
  - maintaining control of the allocation and transfer within their unit
  - 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, Chromebooks, mobile devices and removable data storage devices. Please refer to the relevant sections of this document when considering storing or transferring personal or confidential data

- All activities carried out on school systems and hardware will be monitored in accordance with the general policy

- Staff must ensure that all school data is stored on the school network, and not kept solely on the laptop. Any equipment where personal data is likely to be stored must be encrypted
- Equipment must be kept physically secure in accordance with this policy to be covered for insurance purposes. When travelling by car, best practice is to place the laptop in the boot of the car before starting a journey
- Synchronise all locally stored data, including diary entries, with the central school network server on a frequent basis
- 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 ICT support
- In areas where there are likely to be members of the general public present, 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

Chromebooks

Chromebooks are small, portable laptop devices using Google Chrome Operating System. Chromebooks are enrolled onto the school's Google domain to allow management and control of the devices. Chromebooks are not vulnerable to viruses. All Chromebook internet traffic is monitored and filtered through Impero. Chromebooks are used with Google Workspace for teaching and learning in school.

Chromebook Student Expectations

- Students must follow the school's acceptable use policy when using a Chromebook
- Students are expected to take good care of their Chromebook including protecting it from liquids and unnecessary shocks
- Students are expected to report any damage or problems to their teacher.
- Charging the Chromebook should only be carried out using the supplied or approved power charging unit

Chromebook Teacher Expectations

- Teachers are expected to monitor the use of Chromebooks in lessons and around the school and ensure all usage is focused on learning
- If a teacher becomes aware of any inappropriate use of Chromebooks, e.g. inappropriate messaging using email or school documents, playing of games or other access to inappropriate websites, they should report it to the Head of Year or the Designated Senior Lead and e-Safety Coordinator for investigation. Any websites deemed inappropriate will be blocked on the school network.

Mobile Technologies

Many emerging technologies offer new opportunities for teaching and learning including a move towards personalised learning and 1:1 device ownership for children and young people. Mobile technologies such Smartphones, Smart Watches, iPads, games players, are generally very familiar to children outside of school. They often provide a collaborative, well-known device with possible internet access and thus open up risk and misuse associated with communication and internet use. Emerging technologies will be examined for educational benefit and the risk assessed before use in school is allowed. Our school chooses to manage the use of these devices in the following ways so that users exploit them appropriately.

Personal Mobile Devices (including phones)

- The school allows staff to bring in personal mobile phones and devices for their own use.
- Pupils are allowed to bring personal mobile devices / phones to school but must not use them for personal purposes between 8.30 am and 3.10 pm or whilst on the school site. At all times the device must be switched to silent mode
- This technology may be used for educational purposes, as mutually agreed with the Headteacher. The device user, in this instance, must always ask the prior permission of the bill payer
- 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, video 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)

- The sending of inappropriate text messages between any member of the school community is not allowed
- Permission must be sought before any image, video or sound recordings are made on the devices of any member of the school community
- 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 Onsite backups are replicated to an encrypted remote back up server daily

Social Media, including Facebook Twitter, Instagram, TikTok, Snapchat, Discord

Facebook, Twitter, Instagram, TikTok, Snapchat, Discord and other forms of social media are increasingly becoming an important part of our daily lives.

- Staff are able to setup Learning Platform accounts, using their school email address, in order to be able to teach or educate pupils
- Pupils are not permitted to access their social media accounts whilst at school
- Students in year 12 and 13 are permitted to access their personal social media account using their own device (i.e. mobile phone) but only in the sixth form area
- Staff, pupils, 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, pupils, 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, pupils, 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
- Ensure you remove portable media from your computer when it is left unattended
- 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
- 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, images or video that are not part of the school's business activities; sexual comments or images, video, 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) to be recycled, discarded or otherwise removed from the school site 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. 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.

Appendix 1: Acceptable Use Agreement: Pupils - Secondary

- I will only use ICT systems in school, including the internet, e-mail, digital video, and mobile technologies for school purposes
- I will not download or install software on school technologies
- I will not use removable media (such as USB drives) unless there is no other alternative. I understand that it is my duty to inform the Network Staff and hand over the media device for checking
- I will only log on to the school network, other systems and resources with my own user name and password
- I will follow the school's ICT security system and not reveal my passwords to anyone and change them regularly.
- I will only use my school e-mail address
- I will make sure that all ICT communications with pupils, teachers or others is responsible and sensible
- I will be responsible for my behaviour when using the Internet. This includes resources I access and the language I use
- I will not browse, download, upload or forward material that could be considered offensive or illegal. If I accidentally come across any such material, I will report it immediately to my teacher
- I will not give out any personal information such as name, phone number or address. I will not arrange to meet someone unless this is part of a school project approved by my teacher
- I am aware that when I take images or video of pupils and/ or staff, that I must only store and use these for school purposes in line with school policy and must never distribute these outside the school network without the permission of all parties involved, including in school breaks and all occasions when you are in school uniform or when otherwise representing the school
- I will ensure that my online activity, both in school and outside school, will not cause my school, the staff, pupils or others distress or bring the school community into disrepute, including through uploads of images, video, sounds or texts
- I will support the school approach to online safety and not upload or add any images, video, sounds or text that could upset any member of the school community
- I will respect the privacy and ownership of others' work on-line at all times
- I will not attempt to bypass the internet filtering system
- I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available to my teachers
- I understand that these rules are designed to keep me safe and that if they are not followed, school sanctions will be applied, and my parent/carer may be contacted

Pupils and parents also sign the home-school agreement on entry to the school

- Create family rules for responsible and safe use of the internet and monitor my son/daughter's use of the internet
- Support the school approach to online safety and ensure my son/daughter does not upload or add any images, video, sounds or text that could upset or offend any member of the school community
- Ensure ICT and Social Media is used responsibly at home and support the anti-cyberbullying approach

Appendix 2: Use Agreement: Staff

ICT (including data) and the related technologies such as e-mail, the internet and mobile devices are an expected part of our daily working life in school. This policy is designed to ensure that all staff are aware of their professional responsibilities when using any form of ICT. All staff are expected to sign this policy and always adhere to its contents. Any concerns or clarification should be discussed with name, e-Safety Coordinator or Name, Designated Senior Person.

- I will only use the school's email / Internet / Intranet / Learning Platform and any related technologies for professional purposes or for uses deemed acceptable by the Headteacher or Governing Body
- I will comply with the ICT system security and not disclose any passwords provided to me by the school or other related authorities
- I will ensure that all electronic communications with pupils and staff are compatible with my professional role
- I will not give out my own personal details, such as mobile phone number, personal e-mail address, personal Twitter account, or any other personal social media link, to pupils
- I will only use the approved, secure e-mail system(s) for any school business
- I will ensure that personal data (such as data held on BROMCOM software) is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely. Personal data can only be taken out of school or accessed remotely when authorised by the Headteacher or Governing Body. Personal or confidential data taken off site must be encrypted, e.g. on a password secured laptop or encrypted memory stick
- I will not install any hardware or software without permission of network staff
- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory
- Images or video of pupils and/ or staff will only be taken, stored and used for professional purposes in line with school policy and with written consent of the parent, carer or staff member
- Images or video will not be distributed outside the school network without the permission of the parent/ carer, member of staff or Headteacher
- I will support the school approach to online safety and not upload or add any images, video, sounds or text that could upset any member of the school community
- I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available, on request, to my Line Manager or Headteacher. I will respect copyright and intellectual property rights
- I will ensure that my online activity, both in school and outside school, will not bring the school, my professional role or that of others into disrepute
- I will support and promote the school's e-Safety and Data Security policies and help pupils to be safe and responsible in their use of ICT and related technologies
- I understand this forms part of the terms and conditions set out in my contract of employment

Electronic acceptance is completed by all staff annually. A record is also kept confirming staff acceptance and compliance with the Code of Conduct Policy.

Appendix 3: Acceptable Use Agreement / Code of Conduct Visitor Log

All visitors sign this document on entry to the school.

ICT (including data) and the related technologies such as e-mail, the internet and mobile devices are an expected part of our daily working life in school. This policy is designed to ensure that all visitors are aware of their professional responsibilities when using any form of ICT. All visitors are expected to sign this policy and adhere at all times to its contents. Any concerns or clarification should be discussed with Peter Clift, Deputy Headteacher.

- I will only use the school's email / Internet / Intranet / Learning Platform and any related technologies for professional purposes or for uses deemed acceptable by the Headteacher or Governing Body
- I will comply with the ICT system security and not disclose any passwords provided to me by the school or other related authorities
- I will ensure that all electronic communications with pupils and staff are compatible with my professional role
- I will only use the approved, secure e-mail system(s) for any school business
- I will ensure that personal data (such as data held on BROMCOM software) is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely. Personal data can only be taken out of school or accessed remotely when authorised by the Headteacher or Governing Body. Personal or confidential data taken off site must be encrypted, e.g on a password secured laptop or encrypted memory stick
- I will not install any hardware or software without permission of network staff
- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory
- Images or video of pupils and/ or staff will only be taken, stored and used for professional purposes in line with school policy and with written consent of the parent, carer or staff member
- Images or video will not be distributed outside the school network without the permission of the parent/ carer, member of staff or Headteacher
- I will support the school approach to online safety and not upload or add any images, video, sounds or text that could upset any member of the school community
- I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available, on request, to my Line Manager or Headteacher. I will respect copyright and intellectual property rights
- I will support and promote the school's e-Safety and Data Security policies and help pupils to be safe and responsible in their use of ICT and related technologies

User Signature

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

Appendix 4: Staff Professional Responsibilities

The ESCP e-Safety subgroup group have produced a clear summary of **professional responsibilities related to the use of ICT** which has been endorsed by unions. To download visit https://traded.enfield.gov.uk/thehub/safeguarding-in-schools/online-safety

PROFESSIONAL RESPONSIBILITIES

When using any form of ICT, including the Internet, in school and outside school

For your own protection we advise that you:

- Ensure all electronic communication with pupils, parents, carers, staff and others is compatible with your professional role and in line with school policies.
- Do not talk about your professional role in any capacity when using social media such as Facebook and YouTube.
- Do not put online any text, image, sound or video that could upset or offend any member of the whole school community or be incompatible with your professional role.
- Use school ICT systems and resources for all school business. This includes your school email address, school mobile phone and school video camera.
- Do not give out your own personal details, such as mobile phone number, personal e-mail address or social network details to pupils, parents, carers and others.
- Do not disclose any passwords and ensure that personal data (such as data held on MIS software) is kept secure and used appropriately.
- Only take images of pupils and/ or staff for professional purposes, in accordance with school policy and with the knowledge of SLT.
- Do not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.
- Ensure that your online activity, both in school and outside school, will not bring your organisation or professional role into disrepute.

You have a duty to report any eSafety incident which may impact on you, your professionalism or your organisation.

Appendix 5 - Current Legislation

Acts Relating to Monitoring of Staff email

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.

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 e-Safety

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 or video of children in the United Kingdom. A child for these purposes is a anyone under the age of 18. Viewing an indecent image of a child on your computer means that you have made a digital image. An image or video 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 1998

http://www.opsi.gov.uk/acts/acts1998/ukpga_19980029_en_

1 ***The Freedom of Information Act 2000***

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

Counter-Terrorism and Security Act 2015 (Prevent), Anti-Radicalisation & Counter-Extremism Guidance

https://www.gov.uk/government/publications/preventing-extremism-in-schools-and-childrens-services

Appendix 6: Online Safety Training Needs – self audit for staff

Online Safety Training Needs Audit	
Name of staff member/volunteer:	**Date:**
Question	**Yes/No (add comments if necessary)**
Do you know the name of the person who has lead responsibility for online safety in school?	
Do you know what you must do if a pupil approaches you with a concern or issue?	
Are you familiar with the school's acceptable use agreement for staff, volunteers, governors and visitors?	
Are you familiar with the school's acceptable use agreement for pupils and parents?	
Do you regularly change your password for accessing the school's ICT systems?	
Are you familiar with the school's approach to tackling cyber-bullying?	
Are there any areas of online safety in which you would like training/further training?	