ICT and Internet Acceptable Use Policy

Approved by:	T Coulthard	**Date:**	July 2024
Last reviewed on:	July 2024		
Next review due by:	July 2026		

SOUTH HAMS FEDERATION
ACCEPTABLE USE OF INTERNET POLICY & ON-LINE SAFETY

Approved: Sept 2024 Review: Sept 2026

Introduction and Aims

ICT is an integral part of the way our Federation works, and is an essential resource for pupils, staff, governors, volunteers and visitors. It supports teaching and learning, pastoral and administrative functions of the schools within the South Hams Federation. Consequently, our schools need to build in the use of these technologies in order to prepare our young people with the skills to access life-long learning and employment.

Information and Communications Technology covers a wide range of resources including; web-based and mobile learning. It is also important to recognise the constant and fast paced evolution of ICT within our society as a whole. Currently the internet technologies children and young people are using both inside and outside of the classroom can include, but not exhaustive to:

- Websites
- Learning Platforms and Virtual Learning Environments
- E-mail and Instant Messaging
- Chat Rooms and Social Networking
- Blogs and Wikis
- Podcasting
- Video Broadcasting
- Music Downloading
- Gaming
- Mobile devices including Smart watches with text, video and/or web functionality

Whilst exciting and beneficial both in and out of the context of education, much ICT, particularly web-based resources, are not consistently policed. All users need to be aware of the range of risks associated with the use of these Internet technologies.

At the schools within the South Hams Federation**,** we understand the responsibility and aim to educate our pupils in On-Line 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.

Schools hold personal data on learners, staff and other people to help them conduct their day-to-day activities. Some of this information is sensitive and could be used by another person or criminal organisation to cause harm or distress to an individual. The loss of sensitive information can result in media coverage, and potentially damage the reputation of the school. This can make it more difficult for our schools to use technology to benefit learners.

Everybody in the Federation has a shared responsibility to secure any sensitive information used in their day to day professional duties and even staff not directly involved in data handling should be made aware of the risks and threats and how to minimise them.

Both this policy and the Acceptable Use Agreement (for all staff, governors, visitors and pupils) are

inclusive of both fixed and mobile technologies provided by the school (such as PCs, laptops, tablets, webcams, whiteboards, digital video equipment, etc); and technologies owned by pupils and staff, but brought onto school premises (such as mobile devices, smart watches/devices and portable media players, etc).

Monitoring

All internet activity is logged by the school's internet provider. These logs may be monitored by authorised school staff and the Federation's ICT partner, SCOMIS.

Breaches

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

Any policy breach is grounds for disciplinary action in accordance with the Federation Disciplinary Procedure. Policy breaches may also lead to criminal or civil proceedings.

Incident Reporting

Any security breaches or attempts, and any unauthorised use or suspected misuse of ICT must be immediately reported to the Data Protection Officer via the Executive Headteacher or the Federation's Data Protection Link Officer.

Key Stage One Pupil Acceptable Use Agreement / On-Line Safety Rules

Dear Parent/Carer

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

The school's policy on the Acceptable Use of Internet & On-Line Safety is available for parents to inspect.

Please read and discuss these On-Line Safety rules with your child and return the slip at the bottom of this page. If you have any concerns or would like some explanation please contact the Executive Headteacher or Head of School.

This is How We Stay Safe When We Use Computers:

I will ask a teacher or suitable adult if I want to use the computers.

I will only use activities that a teacher or suitable adult has told or allowed me to use.

I will take care of the computer and other equipment.

I will only share my usernames and passwords with a teacher or suitable adult.

I will ask for help from a teacher or suitable adult if I am not sure what to do or if I think I have done something wrong.

I will ask for help from a teacher or suitable adult if I see something that upsets me on the screen.

I know that if I break the rules I might not be allowed to use a computer.

Parent/Carer signature
We have discussed this and …….....(child's name) agrees to follow the On-Line Safety rules and to support the safe use of ICT at any of the Schools within the South Hams Federation.

We will support the school approach to on-line safety and not deliberately upload or add any images, sounds or text that could upset or offend any member of the school community.

Parent/ Carer Signature ……..……..……

Class …… Date ……

Key Stage Two Pupil Acceptable Use Agreement / On-Line Safety Rules

Dear Parent/Carer

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

The school's policy on the Acceptable Use of Internet & On-Line Safety is available for parents to inspect.

Please read and discuss these On-Line Safety rules with your child and return the slip at the bottom of this page. If you have any concerns or would like some explanation please contact the Executive Headteacher or Head of School.

- I will only use ICT in school for school purposes.
- I will keep my username and password and secure – I will not share it.
- I will not use my own person devices (mobile phones / smart watches / USB devices etc) in school.
- I will not install or attempt to install or store programmes or apps of any type on any school device, nor will I try to alter computer settings.
- I will not use social media sites in school.
- I will make sure that all ICT contact with other children and adults is responsible, polite and sensible.
- I will not deliberately look for, save or send anything that could be unpleasant or nasty. If I accidentally find anything like this I will tell my teacher immediately.
- I will not give out my own details such as my name, phone number or home address. I will not arrange to meet someone unless this is part of a school project approved by my teacher and a responsible adult comes with me.
- I will be responsible for my behaviour when using ICT because I know that these rules are to keep me safe.
- I will support the school approach to online safety and not deliberately upload or add any images, video, sounds or text that could upset any member of the school community
- I will support the school approach to online safety including extremism and radicalisation.
- I know that my use of ICT can be checked and that my parent/carer contacted if a member of school staff is concerned about my On-Line Safety.

✂----------

Parent/Carer signature

We have discussed this and ……..(child's name) agrees to follow the On-Line Safety rules and to support the safe use of ICT at any of the Schools within the South Hams Federation.

We will support the school approach to on-line safety and not deliberately upload or add any images, sounds or text that could upset or offend any member of the school community.

Parent/ Carer Signature ……..……..……

Class …… Date ……

Staff, Governor and Visitor Acceptable Use Agreement

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

- I will only use the school's email / Internet / Intranet / Learning Platform and any related technologies for professional purposes or for uses deemed 'reasonable' by the Executive Headteacher or Board of Governors.
- 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 not take USB devices that contain personal data off the school premises unless agreed by the Executive Headteacher / Head of School.
- I will ensure that any USB removable media device that is used in school containing personal data must be a school issued encrypted removable media device.
- I will ensure that portable equipment where personal data is likely to be stored is encrypted.
- I will ensure that all electronic communications with pupils and staff are compatible with my professional role.
- I will not give out my own personal details, such as mobile phone number and personal e-mail address, to pupils.
- I will only use the approved, secure e-mail system (Egress) for any school business when emailing personal data outside of the Federation
- I will ensure that personal data (such as data held on SIMS 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 Executive Headteacher or Board of Governors. Personal or sensitive data taken off site must be on an encrypted device.
- I will not install any hardware of software without permission of the Executive Headteacher.
- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.
- Images of pupils and/ or staff will only be taken, stored and used for professional purposes inline with school policy and with written consent of the parent, carer or staff member. Images will not be distributed outside the school network without the permission of the parent/ carer, member of staff or Executive Headteacher. All images taken must be on the school cameras / iPads.
- I will support the school approach to online safety and not deliberately upload or add any images, video, sounds or text that could upset or offend any member of the school community
- I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available, on request, to my Line Manager, Head of School or Executive Headteacher.
- I will respect copyright and intellectual property rights.
- I will ensure that my online activity, both in school and outside school, will not bring my professional role into disrepute.
- I will support and promote the school's On-Line Safety and Data Security policies and help pupils to be safe and responsible in their use of ICT and related technologies.

User Signature

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

Signature …….…….…… Date ……

Full Name …….....

Job Title …….....

Computer Viruses

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

E-Mail

The use of e-mail within most schools is an essential means of communication for both staff and pupils. In the context of school, e-mail should not be considered private. Educationally, e-mail can offer significant benefits including; direct written contact between schools on different projects, be it staff or pupil based, within school or internationally. We recognise that pupils need to understand how to style an e-mail in relation to their age and good network etiquette.

Managing E-Mail

- It is the responsibility of each account holder to keep their password secure. Passwords should include uppercase, lowercase, numbers and characters. 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
- The school requires a standard disclaimer to be attached to all e-mail correspondence, stating that, 'the views expressed are not necessarily those of the school or the LA'. The responsibility for adding this disclaimer lies with the account holder
- All e-mails should be written and checked carefully before sending, in the same way as a letter written on school headed paper
- Pupils may only use school approved accounts on the school system and only under direct teacher supervision for educational purposes
- E-mails created or received as part of your School job will be subject to disclosure in response to a request for information under the Freedom of Information Act 2000 or a Subject Access Request. You must therefore actively manage your e-mail account as follows:
  - Delete all e-mails of short-term value
  - Organise e-mail into folders and carry out frequent house-keeping on all folders and archives
- The forwarding of chain letters is not permitted in school.

- All pupil e-mail users are expected to adhere to the generally accepted rules of network etiquette particularly in relation to the use of appropriate language and not revealing any personal details about themselves or others in e-mail communication, or arrange to meet anyone without specific permission, virus checking attachments

- Pupils must immediately tell a teacher/ trusted adult if they receive an offensive e-mail

- Staff must inform the Executive Headteacher or Head of School if they receive an offensive e-mail

- Pupils are introduced to e-mail as part of the ICT Scheme of Work

- However you access your school e-mail, (whether directly or remotely or on non-school hardware) all the school e-mail policies apply

E-mailing Personal, Sensitive, Confidential or Classified Information

- Assess whether the information can be transmitted by other secure means before using e-mail - e-mailing confidential data is not recommended and should be avoided where possible

- Where your conclusion is that e-mail must be used to transmit such data:

  - Obtain express consent from your manager to provide the information by e-mail

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

    - Verify the details, including accurate e-mail address, of any intended recipient of the information

    - Verify (by phoning) the details of a requestor before responding to e-mail requests for information

    - Do not copy or forward the e-mail to any more recipients than is absolutely necessary

  - Do not send the information to anybody/person whose details you have been unable to separately verify (usually by phone)

  - Send the information as an encrypted 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

In exceptional circumstances, the County Council makes provision for secure data transfers to specific external agencies. Such arrangements are currently in place with:

- Police

- MASH

On-Line Safety

Roles and Responsibilities

As on-Line safety is an important aspect of strategic leadership within the school, the Executive Headteacher and governors have ultimate responsibility to ensure that the policy and practices are embedded and monitored. The named On-Line Safety Co-ordinator in the schools within the South Hams Federation is Mrs Tessa Coulthard. All members of the school community have been made aware of who holds this post. It is the role of the On-Line Safety co-ordinator to keep abreast of current issues and guidance through organisations such as SWGfL, Crown Commercial Service, CEOP (Child Exploitation and Online Protection) and Childnet.

Senior management and Governors are updated by the Executive Headteacher and all governors have an understanding of the issues and strategies within the Federation 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:

- Safeguarding and Child Protection
- Home/School agreements
- Behaviour (including the anti-bullying) policy and PSHE
- Data Protection
- Remote Learning
- Mobile Devices

On-Line Safety in the Curriculum

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

- The school has a framework for teaching internet skills in ICT/ PSHE lessons.
- The school provides opportunities within a range of curriculum areas to teach about On-Line Safety
- Educating pupils on the dangers of technologies that maybe encountered outside school is done informally when opportunities arise and as part of the On-Line 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 and respecting other people's information, images, etc through discussion, modeling and 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; i.e. parent/ carer, teacher/ trusted staff member, or an organisation such as Childline or CEOP report abuse button

- Pupils are taught to critically evaluate materials and learn good searching skills through cross curricular teacher models, discussions and via the ICT curriculum.

On-Line Safety Skills Development for Staff

- New staff receive information on the school's acceptable use policy as part of their induction
- All staff have been made aware of individual responsibilities relating to the safeguarding of children within the context of On-Line 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 On-Line Safety activities and awareness within their curriculum areas

Managing the School On-Line Safety Messages

- We endeavor to embed On-Line Safety messages across the curriculum whenever the internet and/or related technologies are used
- On-Line Safety posters will be prominently displayed

On-Line Safety Incident Reporting

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

On-Line Safety Incident Log

Please see Appendix A. Some incidents may need to be recorded in other places, if they relate to a bullying or racist incident.

Internet Access

The internet is an open communication medium, available to all, at all times. Anyone can view information, send messages, discuss ideas and publish material which makes it both an invaluable resource for education, business and social interaction, as well as a potential risk to young and vulnerable people. All use of the **Grid for Learning** (SWGfL) is logged and the logs are randomly but regularly monitored. Whenever any inappropriate use is detected it will be followed up.

Managing the Internet

- Pupils have supervised access to internet resources (where reasonable) through the school's fixed and mobile internet technology
- Staff will preview any recommended sites before use

- Raw image searches are discouraged when working with pupils

- If internet research is set for homework, specific sites will be suggested that have previously been checked by the teacher. It is advised that parents recheck these sites and supervise this work. Parents will be advised to supervise any further research

- All users must observe software copyright at all times. It is illegal to copy or distribute school software or illegal software from other sources

- All users must observe copyright of materials from electronic resources

Internet Use

- You must not post personal, sensitive, confidential or classified information or disseminate such information in any way that may compromise its intended restricted audience

- Don't reveal names of colleagues, customers or clients or any other confidential information acquired through your job on any social networking site or blog

- On-line gambling or gaming is not allowed

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

Infrastructure

- Local Authority has a monitoring solution via the Grid for Learning where web-based activity is monitored and recorded

- School internet access is controlled through the LA's web filtering service.

- Staff and pupils are aware that school based email and internet activity can be monitored and explored further if required

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

- It is the responsibility of the schools within the Federation, to ensure that Anti-virus protection is installed and kept up-to-date on all school machines

- Pupils and Staff using personal removable media are responsible for measures to protect against viruses, for example making sure that additional systems used have up-to-date virus protection software. It is not the school's responsibility 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 teacher 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 Executive Headteacher

- If there are any issues related to viruses or anti-virus software, the ICT Lead / external provider should be informed

Remote access

We allow staff to access the school's ICT facilities and materials remotely. Staff should ensure use of any personal network is secure. Staff are able to access the school shared drives via their school email login and should each time they leave their laptop they logout.

Staff accessing the school's ICT facilities and materials remotely must abide by the same rules as those accessing the facilities and materials on-site. Staff must be particularly vigilant if they use the school's ICT facilities outside the school and take such precautions whilst using school equipment remotely against importing viruses or compromising system security. Staff should make the Executive Headteacher/Head of School and ICT provider aware of any such compromise.

Our ICT facilities (email / school drives) contain information which is confidential and/or subject to data protection legislation. Such information must be treated with extreme care and in accordance with our Data Protection policy.

School Social Media Accounts

The Federation has an official Facebook and Twitter/ 'X' page managed by the Federation's HR team. Staff members who have not been authorised to manage, or post to the account, must not access, or attempt to access the account.

Cyber Security

Please see the glossary to help understand cyber security terminology.

The school will:

- Work with governors, ICT provider and DPO to make sure cyber security is given the time and resources it needs to make the school secure
- Provide Cyber training for new and current staff on the basics of cyber security via the National Cyber Security Centre.
- Make sure staff are aware of its procedures for reporting and responding to cyber security incidents
- Investigate with our ICT provider whether our IT software needs updating or replacing to be more secure
- Not engage in ransom requests from ransomware attacks, as this would not guarantee recovery of data
- Back up critical data and store securely off the Cloud drives
- Delegate specific responsibility for maintaining the security of our management information system (MIS). Currently this responsibility is via our ICT and MIS provider SCOMIS.

Make sure staff:

- Dial into our network using a virtual private network (VPN) when working from home
- Enable multi-factor authentication where they can, on things like school email accounts
- Store passwords securely
- Develop, review and test an incident response/emergency management plan including how the Federation will communicate with everyone if communications go down. The Executive Headteacher will be responsible for notifying the Local Authority, Police and Action Fraud of the incident.

Managing Other Web 2 Technologies

Web 2, 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 denies access to social networking sites to pupils within school
- All pupils are advised to be cautious about the information given by others on sites, for example users not being who they say they are
- Pupils are taught to avoid placing images of themselves (or details within images that could give background details) on such sites and to consider the appropriateness of any images they post due to the difficulty of removing an image once online
- Pupils are always reminded to avoid giving out personal details on such sites which may identify them or where they are (full name, address, mobile/ home phone numbers, school details, IM/ email address, specific hobbies/ interests)
- Our pupils are advised to set and maintain profiles on such sites to maximum privacy and deny access to unknown individuals
- Pupils are encouraged to be wary about publishing specific and detailed private thoughts online
- Our pupils are asked to report any incidents of bullying to the school
- Staff may only create blogs, wikis or other web 2 spaces in order to communicate with pupils using the LA Learning Platform or other systems approved by the Executive Headteacher

Parental Involvement

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

- Parents/carers are asked to read through and sign Acceptable Use Agreements on behalf of their child on admission to school at Key Stage 1 and again at Key Stage 2.
- Parents/carers are required to make a decision as to whether they consent to images of their child being taken/ used in the public domain (e.g., on school website)
- Parents/carers are expected to sign a Pupil Acceptable Use Agreement containing the following statement or similar
    - → **We will support the school approach to on-line safety and not deliberately upload or add any images, sounds or text that could upset or offend any member of the school community**
- The school disseminates information to parents relating to On-Line Safety where appropriate in the form of;

- Information and celebration events
- Posters
- Website
- Newsletter items

Passwords and Password Security

Passwords

- Always use your own personal passwords to access computer based services
- 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
- Passwords must contain a minimum of six characters, uppercase, lower case and symbols and be difficult to guess
- User ID and passwords for staff and pupils who have left the School are removed from the system

If you think your password may have been compromised or someone else has become aware of your password report this to the Business Manager.

Password Security

Password security is essential for staff, particularly as they are able to access and use pupil data. Staff are expected to have secure passwords which are not shared with anyone. The pupils are expected to keep their passwords secret and not to share with others, particularly their friends. Staff and pupils are regularly reminded of the need for password security.

- All users read and sign an Acceptable Use Agreement to demonstrate that they have understood the school's On-Line Safety Policy and Data Security
- Staff are aware of their individual responsibilities to protect the security and confidentiality of school networks, MIS systems, including ensuring that passwords are not shared and are changed periodically. Individual staff users must also make sure that workstations are not left unattended and are locked.

Safe Use of Images

Taking of Images and Film

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

- With the written consent of parents (on behalf of pupils) and staff, the school permits the appropriate taking of images by staff and pupils with school equipment
- Staff are not permitted to use personal digital equipment, such as mobile phones and cameras, to record images of pupils, this includes when on field trips.
- Pupils are not permitted to use personal digital equipment, including mobile phones and cameras, to record images of the others, this includes when on field trips.

Consent of Adults Who Work at the School

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

Publishing Pupil's Images and Work

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

- on the schools and federation web sites
- on the school weekly newsletters
- on printed publications that the school may produce for promotional purposes
- recorded/ transmitted on a video or webcam
- in display material that may be used in the school's communal areas
- in display material that may be used in external areas, ie exhibition promoting the school
- general media appearances, eg local/ national media/ press releases sent to the press highlighting an activity (sent using traditional methods or electronically)

Parents will be asked annually whether they wish to update their consent.

Parents/ carers may withdraw permission, in writing, at any time.

Pupils' names will not be published alongside their image and vice versa. E-mail and postal addresses of pupils will not be published. Pupils' full names will not be published.

Before posting pupil work on the Internet, a check needs to be made to ensure that permission has been given for work to be displayed.

Only the Web Manager / SLT and HR team & Schools Admin have authority to upload to the site.

Storage of Images

- Images/ films of children are stored on the school's network / secure drives.
- Pupils and staff are not permitted to use personal portable media for storage of images (eg USB sticks) without the express permission of the Executive Headteacher
- Rights of access to this material are restricted to the teaching staff and pupils within the confines of the school network

Teachers have the responsibility of deleting the images when they are no longer required, or the pupil has left the school

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

School ICT Equipment

- As a user of ICT, you are responsible for any activity undertaken on the school's ICT equipment provided to you
- It is recommended that schools log ICT equipment issued to staff and record serial numbers 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 that you save your data on a frequent basis to the school's network cloud drives. You are responsible for the backup and restoration of any of your data that is not held on the school's network cloud drives
- Personal or sensitive data should not be stored on the local drives of desktop PCs by on personal cloud network drives. 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 (devices must time out after 4 minutes of inactive use. Any PCs etc 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 to access the school server or confidential information recorded on SIMS.
- On termination of employment, resignation or transfer, return all ICT equipment to your Manager. 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 removable media equipment 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. 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 and iPads. Please refer to the relevant sections of this document when considering storing or transferring personal or sensitive data

- All activities carried out on School systems and hardware will be monitored in accordance with the general policy
- Staff must ensure that all school data is stored on school's network cloud drives, 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 your car before starting your journey
- Synchronise all locally stored data, including diary entries, on a frequent basis
- Ensure portable and mobile ICT equipment is made available as and when requested. Where possible our ICT external provider/partner (SCOMIS) will upload details of school portable devices to the Cloud Admin consoles so that they can be routinely monitored and ensuring that all necessary updates for anti-virus and software installations, patches or upgrades have been applied.
- The installation of any applications or software packages must be authorised by the ICT Lead and Executive Headteacher, 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

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

Personal Mobile Devices (including phones)

- Please refer to the Federation's mobile device policy.

Removable Media

The use of removable media is strongly discouraged and staff are prohibited from taking removable media devices that contain personal data off school premises. If storing/transferring personal, sensitive, confidential or classified information using Removable Media within school the following should be adhered to:

- Only use school issued encrypted removable media devices
- Store all removable media securely
- Removable media must be disposed of securely

Smile and Stay Safe Poster

On-Line Safety guidelines to be displayed throughout the school

SMILE and Stay Safe

Staying safe means keeping your personal details private. Such as full name, phone number, home address, photos or school. Never reply to ASL (age, sex, location)

Meeting up with someone you have met online can be dangerous. Only meet up if you have first told your parent or carer and they can be with you.

Information online can be untrue, biased or just inaccurate. Someone online may not be telling the truth about who they are - they may not be a 'friend'

Let a parent, carer, teacher or trusted adult know if you ever feel worried, uncomfortable or frightened about something online or someone you have met or who has contacted you online.

Emails, downloads, IM messages, photos and anything from someone you do not know or trust may contain a virus or unpleasant message. So do not open or reply.

Glossary of cyber security terminology

These key terms will help you to understand the common forms of cyber attack and the measures the school will put in place. They're from the National Cyber Security Centre (NCSC) glossary.

TERM	DEFINITION
Antivirus	Software designed to detect, stop and remove malicious software and viruses.
Cloud	Where you can store and access your resources (including data and software) via the internet, instead of locally on physical devices.
Cyber attack	An attempt to access, damage or disrupt your computer systems, networks or devices maliciously.
Cyber incident	Where the security of your system or service has been breached.
Cyber security	The protection of your devices, services and networks (and the information they contain) from theft or damage.
Download attack	Where malicious software or a virus is downloaded unintentionally onto a device without the user's knowledge or consent.
Firewall	Hardware or software that uses a defined rule set to constrain network traffic – this is to prevent unauthorised access to or from a network.
Hacker	Someone with some computer skills who uses them to break into computers, systems and networks.
Malware	Malicious software. This includes viruses, trojans or any code or content that can adversely impact individuals or organisations.
Patching	Updating firmware or software to improve security and/or enhance functionality.
Pentest	Short for penetration test. This is an authorised test of a computer network or system to look for security weaknesses.
Phishing	Untargeted, mass emails sent to many people asking for sensitive information (like bank details) or encouraging them to visit a fake website.
Ransomware	Malicious software that stops you from using your data or systems until you make a payment.
Social engineering	Manipulating people into giving information or carrying out specific actions that an attacker can use.

TERM	DEFINITION
Spear-phishing	A more targeted form of phishing where an email is designed to look like it's from a person the recipient knows and/or trusts.
Trojan	A type of malware/virus designed to look like legitimate software that can be used to hack a victim's computer.
Two-factor/multi-factor authentication	Using 2 or more different components to verify a user's identity.
Virus	Programs designed to self-replicate and infect legitimate software programs or systems.
Virtual Private Network (VPN)	An encrypted network which allows remote users to connect securely.
Whaling	Highly targeted phishing attacks (where emails are made to look legitimate) aimed at senior executives.

Review Procedure

There will be an on-going opportunity for staff to discuss with the Executive Headteacher any issue of On-Line Safety that concerns them

This policy will be reviewed every 2 years and consideration given to the implications for future whole federation 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 has been read, amended and approved by the Executive Headteacher and Governors in July 2024.