

ICT and internet acceptable use policy

Percy Hedley School

Policy Name: ICT and Internet Acceptable Use Policy	Issue Date: July 2026	Version No: 4
Status: Approved	Next Review Date: July 2027	Page 1 of 38

Policy Control/Monitoring

Approved by: (Position in Organisation)	Director of Education
Date (dd/mm/yyyy):	13/07/2026
Accountability: (Position in Organisation)	Computing Lead
Revision Cycle:	Annual
Brief details of amendments made	Accountability. AI tool update. Filtering and Monitoring devices.

Equality Impact Assessment

The Foundation’s commitment is to create a positive culture of respect for all staff and service users and to identify, remove or minimise risks of unlawful discrimination and disadvantage in its policies, functions and activities. As part of its development this document has been assessed in line with The Foundation’s equality impact assessment procedure.

Version Control Tracker

Version Number	Date
1	July 2023
2	15 th July 2024
3	July 2025

Policy Name: ICT and Internet Acceptable Use Policy	Issue Date: July 2026	Version No: 4
Status: Approved	Next Review Date: July 2027	Page 2 of 38

Version Number	Date
4	July 2026

Policy Name: ICT and Internet Acceptable Use Policy	Issue Date: July 2026	Version No: 4
Status: Approved	Next Review Date: July 2027	Page 3 of 38

1. Introduction

Information and communications technology (ICT) is an integral part of the way our school works, and is a critical resource for pupils, staff (including the senior leadership team), governors, volunteers and visitors. It supports teaching and learning, and the pastoral and administrative functions of the school.

However, the ICT resources and facilities our school uses could also pose risks to data protection, online safety and safeguarding.

This policy includes:

- The purpose of the ICT and Internet Acceptable Use Policy.
- The scope of the ICT and Internet Acceptable Use Policy.
- Key definitions
- The principles of the ICT and Internet Acceptable Use Policy.
- Monitoring and compliance of the ICT and Internet Acceptable Use Policy.
- Associated policies and references, including relevant legislation and guidance.

[Appendix 1: Facebook cheat sheet for staff](#)

[Appendix 2: Acceptable use of the internet: agreement for parents and carers](#)

[Appendix 3: Acceptable use agreement for older pupils](#)

[Appendix 4: Acceptable use agreement for younger pupils](#)

[Appendix 5: Acceptable use agreement for staff, governors, volunteers and visitors](#)

[Appendix 6: Glossary of cyber security terminology](#)

2. Purpose

This policy aims to:

- Set guidelines and rules on the use of school ICT resources for staff, pupils, parents/carers and governors
- Establish clear expectations for the way all members of the school community engage with each other online
- Support the school's policies on data protection, online safety and safeguarding
- Prevent disruption that could occur to the school through the misuse, or attempted misuse, of ICT systems
- Support the school in teaching pupils safe and effective internet and ICT use

This policy covers all users of our school's ICT facilities, including governors, staff, pupils, volunteers, contractors and visitors.

Breaches of this policy may be dealt with under our behaviour support policy and procedure/staff code of conduct.

Policy Name: ICT and Internet Acceptable Use Policy	Issue Date: July 2026	Version No: 4
Status: Approved	Next Review Date: July 2027	Page 4 of 38

3. Scope

Data security

The school is responsible for making sure it has the appropriate level of security protection and procedures in place to safeguard its systems, staff and learners. It therefore takes steps to protect the security of its computing resources, data and user accounts. The effectiveness of these procedures is reviewed periodically to keep up with evolving cybercrime technologies.

Staff, pupils, parents/carers and others who use the school's ICT facilities should use safe computing practices at all times. We aim to meet the cyber security standards recommended by the Department for Education's guidance on [digital and technology standards in schools and colleges](#), including the use of:

- Firewalls
- Security features
- User authentication and multi-factor authentication
- Anti-malware software

Passwords

All users of the school's ICT facilities will be issued strong passwords for their accounts from the IT department and keep these passwords secure.

Users are responsible for the security of their passwords and accounts, and for setting permissions for accounts and files they control.

Members of staff or pupils who disclose account or password information may face disciplinary action. Parents, visitors or volunteers who disclose account or password information may have their access rights revoked.

Software updates, firewalls and anti-virus software

All of the school's ICT devices that support software updates, security updates and anti-virus products will have these installed and be configured to perform such updates regularly or automatically.

Users must not circumvent or make any attempt to circumvent the administrative, physical and technical safeguards we implement and maintain to protect personal data and the school's ICT facilities.

Any personal devices using the school's network must all be configured in this way.

Data protection

All personal data must be processed and stored in line with data protection regulations and the school's data protection policy.

Please see the school's data protection policy, foundation policies, PHF connect.

Policy Name: ICT and Internet Acceptable Use Policy	Issue Date: July 2026	Version No: 4
Status: Approved	Next Review Date: July 2027	Page 5 of 38

Access to facilities and materials

All users of the school's ICT facilities will have clearly defined access rights to school systems, files and devices.

These access rights are managed by the IT Team.

Users should not access, or attempt to access, systems, files or devices to which they have not been granted access. If access is provided in error, or if something a user should not have access to is shared with them, they should alert the IT Team immediately.

Users should always log out of systems and lock their equipment when they are not in use to avoid any unauthorised access. Equipment and systems should always be logged out of and shut down completely at the end of each working day.

Encryption

The school makes sure that its devices and systems have an appropriate level of encryption.

School staff may use personal phones, computers and mobile devices to access school data held in the cloud, however the devices must meet minimum security requirements relating to encryption and (in some cases) install additional management software.

The use of portable storage devices (e.g. USB hard drives) are strictly controlled by the IT Team, with only approved encrypted devices being accessible.

Protection from cyber attacks

Please see the glossary (appendix 6) to help you understand cyber security terminology.

The school will:

- Work with governors and the IT Team to make sure cyber security is given the time and resources it needs to make the school secure
- Provide annual training for staff (and include this training in any induction for new starters, if they join outside of the school's annual training window) on the basics of cyber security, including how to:
 - Check the sender address in an email
 - Respond to a request for bank details, personal information or login details
 - Verify requests for payments or changes to information
- Make sure staff are aware of its procedures for reporting and responding to cyber security incidents
- Investigate 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
- Put controls in place that are:
 - **Proportionate:** the school will verify this using a third-party audit (such as [360 degree safe](#)) annually, to objectively test that what it has in place is effective

Policy Name: ICT and Internet Acceptable Use Policy	Issue Date: July 2026	Version No: 4
Status: Approved	Next Review Date: July 2027	Page 6 of 38

- **Multi-layered:** everyone will be clear on what to look out for to keep our systems safe
- **Up to date:** with a system in place to monitor when the school needs to update its software
- **Regularly reviewed and tested:** to make sure the systems are as effective and secure as they can be
- Back up critical data, with data held on the shared drive backed up daily and long-term weekly backups held on tape for 12 months.
- Delegate specific responsibility for maintaining the security of our management information system (MIS) to ESS SIMS.
- 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
 - Are aware of IT security good practice such as using appropriate passwords and spotting phishing emails
- Ensure that the Foundation's network is protected at all times by a modern and up-to-date firewall
- Check that its supply chain is secure, for example by asking suppliers about how secure their business practices are and checking if they have the [Cyber Essentials](#) certification
- Work with partner organisations including JISC and NCSC to see what they can offer the school regarding cyber security, such as advice on which service providers to use or assistance with procurement

Internet access

The school's wireless internet connection is secure.

All Foundation computers and mobile devices are set up to use a dedicated staff wireless network. Passwords for joining this network are not shared.

A guest/public wireless connection is available which only allows internet access and can be signed up for 24hrs at a time. It is NOT intended to be used by staff or students.

All wireless connections are subject to the same monitoring and filtering outlined in section 5.5.

We are aware that web filtering is not foolproof. If a member of staff encounters a website which is blocked and should not be, or they believe should be blocked in future, they should report this to the DSL who can confirm this and request the IT Team make the appropriate change.

Pupils

Computers and mobile devices owned and used by students (e.g. communication devices) can be connected to a separate wireless network that allow internet access, but no access to staff resources such as the shared drive. Access can be arranged by contacting the IT Team.

Policy Name: ICT and Internet Acceptable Use Policy	Issue Date: July 2026	Version No: 4
Status: Approved	Next Review Date: July 2027	Page 7 of 38

Parents/carers and visitors

Parents/carers and visitors to the school will not be permitted to use the school's WiFi unless specific authorisation is granted by the Business Manager or DSL team.

The headteacher will only grant authorisation if:

- Parents/carers are working with the school in an official capacity (e.g. as an employee, as a volunteer or as a member of the FOPHS)
- Visitors need to access the school's WiFi in order to fulfil the purpose of their visit (for instance, to access materials stored on personal devices as part of a presentation or lesson plan)

4. Definitions

- **ICT facilities:** all facilities, systems and services including, but not limited to, network infrastructure, desktop computers, laptops, tablets, phones, music players or hardware, software, websites, web applications or services, and any device system or service that may become available in the future which is provided as part of the school's ICT service
- **Users:** anyone authorised by the school to use the school's ICT facilities, including governors, staff, pupils, volunteers, contractors and visitors
- **Personal use:** any use or activity not directly related to the users' employment, study or purpose agreed by an authorised user
- **Authorised personnel:** employees authorised by the school to perform systems administration and/or monitoring of the ICT facilities
- **Materials:** files and data created using the school's ICT facilities including but not limited to documents, photos, audio, video, printed output, web pages, social networking sites and blogs

See appendix 6 for a glossary of cyber security terminology.

5. Principles

Unacceptable use

The following is considered unacceptable use of the school's ICT facilities. Any breach of this policy may result in disciplinary or behaviour proceedings (see section 4.2 below).

Unacceptable use of the school's ICT facilities includes:

- Using the school's ICT facilities to breach intellectual property rights or copyright
- Using the school's ICT facilities to bully or harass someone else, or to promote unlawful discrimination
- Breaching the school's policies or procedures
- Any illegal conduct, or statements which are deemed to be advocating illegal activity
- Online gambling, inappropriate advertising, phishing and/or financial scams
- Accessing, creating, storing, linking to or sending material that is pornographic, offensive, obscene or otherwise inappropriate or harmful

Policy Name: ICT and Internet Acceptable Use Policy	Issue Date: July 2026	Version No: 4
Status: Approved	Next Review Date: July 2027	Page 8 of 38

- Consensual and non-consensual sharing of nude and semi-nude images and/or videos and/or livestreams
- Activity which defames or disparages the school, or risks bringing the school into disrepute
- Sharing confidential information about the school, its pupils, or other members of the school community
- Connecting any device to the school's ICT network without approval from authorised personnel
- Setting up any software, applications or web services on the school's network without approval by authorised personnel, or creating or using any programme, tool or item of software designed to interfere with the functioning of the school's ICT facilities, accounts or data
- Gaining, or attempting to gain, access to restricted areas of the network, or to any password-protected information, without approval from authorised personnel
- Allowing, encouraging or enabling others to gain (or attempt to gain) unauthorised access to the school's ICT facilities
- Causing intentional damage to the school's ICT facilities
- Removing, deleting or disposing of the school's ICT equipment, systems, programmes or information without permission from authorised personnel
- Causing a data breach by accessing, modifying, or sharing data (including personal data) to which a user is not permitted by authorised personnel to have access, or without authorisation
- Using inappropriate or offensive language
- Promoting a private business, unless that business is directly related to the school
- Using websites or mechanisms to bypass the school's filtering or monitoring mechanisms
- Engaging in content or conduct that is radicalised, extremist, racist, antisemitic or discriminatory in any other way
- Using AI tools and generative chatbots (such as ChatGPT and Google Bard):
 - During assessments, including internal and external assessments, and coursework
 - To write their homework or class assignments, where AI-generated text or imagery is presented as their own work

This is not an exhaustive list. The school reserves the right to amend this list at any time. The headteacher, DSL or Computing DSL will use their professional judgement to determine whether any act or behaviour not on the list above is considered unacceptable use of the school's ICT facilities.

Exceptions from unacceptable use

Where the use of school ICT facilities (on the school premises and/or remotely) is required for a purpose that would otherwise be considered an unacceptable use, exemptions to the policy may be granted at the headteacher's discretion. Any AI use should be sanctioned by the subject teacher who is involved with the group at the time.

Under some circumstances approval can be granted, for example:

- Pupils may use AI tools and generative chatbots:

Policy Name: ICT and Internet Acceptable Use Policy	Issue Date: July 2026	Version No: 4
Status: Approved	Next Review Date: July 2027	Page 9 of 38

- As a research tool to help them find out about new topics and ideas
- When specifically studying and discussing AI in schoolwork, for example in IT lessons or art homework about AI-generated images. All AI-generated content must be properly attributed

Sanctions

Pupils and staff who engage in any of the unacceptable activities listed above may face disciplinary action in line with the school's policies on behaviour support policy & procedure/staff code of conduct/etc.

Refusal to comply could result in the revoke of use of the Percy Hedley Wi-Fi and PHS owned devices.

Staff (including governors, volunteers, and contractors)

Access to school ICT facilities and materials

The school's IT Team manages access to the school's ICT facilities and materials for school staff. That includes, but is not limited to:

- Computers, tablets, mobile phones and other devices
- Access permissions for certain programmes or files

Staff will be provided with unique login/account information and passwords that they must use when accessing the school's ICT facilities.

Staff who have access to files that they are not authorised to view or edit, or who need their access permissions updated or changed, should contact the IT Team.

Use of phones and email

The school provides each member of staff with an email address.

This email account should be used for work purposes only. Staff should enable multi-factor authentication on their email account(s).

All work-related business should be conducted using the email address the school has provided.

Staff must not share their personal email addresses with parents/carers and pupils and must not send any work-related materials using their personal email account.

Staff must take care with the content of all email messages, as incorrect or improper statements can give rise to claims for discrimination, harassment, defamation, breach of confidentiality or breach of contract.

Email messages are required to be disclosed in legal proceedings or in response to requests from individuals under the Data Protection Act 2018 in the same way as paper documents. Deletion from a user's inbox does not mean that an email cannot be recovered for the purposes of disclosure. All email messages should be treated as potentially retrievable.

Policy Name: ICT and Internet Acceptable Use Policy	Issue Date: July 2026	Version No: 4
Status: Approved	Next Review Date: July 2027	Page 10 of 38

Staff must take extra care when sending sensitive or confidential information by email. Any attachments containing sensitive or confidential information should be encrypted so that the information is only accessible by the intended recipient.

If staff receive an email in error, the sender should be informed and the email deleted. If the email contains sensitive or confidential information, the user must not make use of that information or disclose that information.

If staff send an email in error that contains the personal information of another person, they must inform the Data Protection Officer immediately and follow our data breach procedure.

Staff must not give their personal phone number(s) to parents/carers or pupils. Staff must use phones provided by the school to conduct all work-related business.

School phones must not be used for personal matters.

Staff who are provided with mobile phones as equipment for their role must abide by the same rules for ICT acceptable use as set out in section 4.

Staff who would like to record a phone conversation should speak to the lead designated safeguarding officer.

All non-standard recordings of phone conversations must be pre-approved, and consent obtained from all parties involved.

For instance:

- Discussing a complaint raised by a parent/carer or member of the public
- Calling parents/carers to discuss behaviour or sanctions
- Taking advice from relevant professionals regarding safeguarding, special educational needs (SEN) assessments, etc.
- Discussing requests for term-time holidays

Personal use

Staff are permitted to occasionally use school ICT facilities for personal use, subject to certain conditions set out below. This permission must not be overused or abused. The Senior Leadership Team may withdraw or restrict this permission at any time and at their discretion.

Personal use is permitted provided that such use:

- Does not take place during non-break time
- Does not constitute 'unacceptable use', as defined in section 4
- Takes place when no pupils are present
- Does not interfere with their jobs, or prevent other staff or pupils from using the facilities for work or educational purposes

Policy Name: ICT and Internet Acceptable Use Policy	Issue Date: July 2026	Version No: 4
Status: Approved	Next Review Date: July 2027	Page 11 of 38

Staff may not use the school's ICT facilities to store personal, non-work-related information or materials (such as music, videos or photos).

Staff should be aware that use of the school's ICT facilities for personal use may put personal communications within the scope of the school's ICT monitoring activities (see section 5.5). Where breaches of this policy are found, disciplinary action may be taken.

Staff are also permitted to use their personal devices (such as mobile phones or tablets) in line with the school's mobile phone/personal device policy.

Staff should be aware that personal use of ICT (even when not using school ICT facilities) can impact on their employment by, for instance, putting personal details in the public domain, where pupils and parents/carers could see them.

Staff should take care to follow the school's guidelines on use of social media (see appendix 1 social media policy on: foundation policies, PHF connect and use of email (see section 5.1.1) to protect themselves online and avoid compromising their professional integrity.

Personal social media accounts

Members of staff should make sure their use of social media, either for work or personal purposes, is appropriate at all times.

The school has guidelines for staff on appropriate security settings for Facebook accounts (see appendix 1).

Remote access

We allow staff to access the school's ICT facilities and materials remotely.

Sonicwall NetExtender is made available on all Foundation laptops and staff have access to use this service when working off-site and requiring access to electronic materials and systems (e.g. the shared drive and SIMS). Use of NetExtender requires setting up multi-factor authentication. Instructions for setting up and using NetExtender are available on PHF Connect.

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 must take such precautions as the Head of Technology may require against importing viruses or compromising system security.

Our ICT facilities 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 school has an official Facebook account, managed by the Family Liaison officer and Business Manager. Staff members who have not been authorised to manage, or post to, the account must not access or attempt to access, the account. This is a closed group for the friends of Percy Hedley School.

Policy Name: ICT and Internet Acceptable Use Policy	Issue Date: July 2026	Version No: 4
Status: Approved	Next Review Date: July 2027	Page 12 of 38

The school has guidelines for what may and must not be posted on its social media accounts. Those who are authorised to manage, or post to, the account must make sure they abide by these guidelines at all times.

Monitoring and filtering of the school network and use of ICT facilities

To safeguard and promote the welfare of children and provide them with a safe environment to learn, the school reserves the right to filter and monitor the use of its ICT facilities and network. This includes, but is not limited to, the filtering and monitoring of:

- Internet sites visited
- Bandwidth usage
- Email accounts
- User activity/access logs
- Any other electronic communications

Only authorised ICT personnel may filter, inspect, monitor, intercept, assess, record and disclose the above, to the extent permitted by law. Notifications of attempts to access inappropriate websites and materials, or the use of concerning search terms on common platforms relating to adult matters, profanities, drugs and extremism will be reported to Safeguarding staff.

Requests to provide information about an individual's usage of ICT, give access to a person's account or carry out detailed investigation will only be accepted with the authorisation of a member of the Foundation Executive, the HR Team, Data Protection Officer or DSL depending on the context and nature of the request.

The school monitors ICT use in order to:

- Obtain information related to school business
- Investigate compliance with school policies, procedures and standards
- Ensure effective school and ICT operation
- Conduct training or quality control exercises
- Prevent or detect crime
- Comply with a subject access request, Freedom of Information Act request, or any other legal obligation

Our governing board is responsible for making sure that:

- The school meets the DfE's [filtering and monitoring standards](#)
- Appropriate filtering and monitoring systems are in place
- Staff are aware of those systems and trained in their related roles and responsibilities
 - For the leadership team and relevant staff, this will include how to manage the processes and systems effectively and how to escalate concerns
- It regularly reviews the effectiveness of the school's monitoring and filtering systems

Policy Name: ICT and Internet Acceptable Use Policy	Issue Date: July 2026	Version No: 4
Status: Approved	Next Review Date: July 2027	Page 13 of 38

The school's designated safeguarding lead (DSL) will take lead responsibility for understanding the filtering and monitoring systems and processes in place.

Where appropriate, staff may raise concerns about monitored activity with the school's DSL and ICT manager, as appropriate.

The school uses SonicTek as its filtering and monitoring provider. This system has been selected because it integrates effectively with the school's existing firewall infrastructure and meets the educational and safeguarding requirements of the school. SonicTek provides WebVue alerts, enabling the school to monitor and respond appropriately to online activity which may indicate safeguarding concerns or breaches of the school's Acceptable Use Policy. Web access blocking lists are automatically maintained by Sonicwall, supplemented by custom whitelist/blacklists maintained by the IT Team.

The filtering system is designed to prevent access to content that is inappropriate, harmful or unlawful. This includes, but is not limited to, websites and online content categorised as:

- Pornography and sexually explicit material
- Racial hatred and discriminatory content
- Extremist or radicalising material
- Gaming and gambling sites where deemed inappropriate for educational use
- Sites promoting or facilitating illegal activities

In addition to blocking inappropriate content, the monitoring functionality can identify and alert staff to potential safeguarding concerns, including indicators relating to:

- Self-harm or suicidal ideation
- Serious violent crime
- County lines exploitation and grooming
- Other behaviours or online activity that may place a child at risk

The school's email system is also subject to filtering and monitoring controls. Email filtering is provided through Microsoft's automated protection systems, supplemented by additional keyword-based filters configured and regularly reviewed by the ICT Manager.

The school's filtering provider utilises regularly updated Internet Watch Foundation (IWF) and Counter-Terrorism Internet Referral Unit (CTIRU) block lists to ensure that known harmful and illegal content is appropriately restricted. The ICT Manager carries out a monthly filtering and monitoring review, which includes verifying that IWF and CTIRU block lists are current, active and being correctly applied. The outcomes of these checks are circulated to relevant services and school leaders as appropriate.

To ensure that filtering and monitoring arrangements remain effective across the school's digital estate, regular testing is carried out on a representative range of devices, including:

Policy Name: ICT and Internet Acceptable Use Policy	Issue Date: July 2026	Version No: 4
Status: Approved	Next Review Date: July 2027	Page 14 of 38

- Staff laptops
- Student laptops
- Desktop computers
- iPads
- Maintenance tablets
- Tablets used for Earwig
- School mobile phones

This list is not intended to be exhaustive. The school reserves the right to include any additional device, platform, service or technology within its filtering and monitoring testing programme where this is considered necessary to support safeguarding, security, compliance or operational requirements.

The school recognises that filtering and monitoring systems form an important part of its safeguarding arrangements but cannot guarantee that all unsuitable material will be blocked. Filtering and monitoring are therefore supported by appropriate supervision, education, staff training and clear reporting procedures to promote safe and responsible use of technology.

Pupils

Access to ICT facilities

ICT facilities are available to pupils, when they are required to specific lessons and in break times/rewards times if appropriate for that pupil. Some pupils have their own Voice output communication aides (Vocas) which should be with them at all times. For example:

- Computers and equipment in the school's ICT suite are available to pupils only under the supervision of staff
- Specialist ICT equipment, such as that used for music, or design and technology, must only be used under the supervision of staff
- Pupils will be provided with an account linked to the school's virtual learning environment, which they can access from any device by using Microsoft teams.

Search and deletion

Under the Education Act 2011, the headteacher, and any member of staff authorised to do so by the headteacher, can search pupils and confiscate their mobile phones, computers or other devices that the authorised staff member has reasonable grounds for suspecting:

- Poses a risk to staff or pupils, **and/or**
- Is identified in the school rules as a banned item for which a search can be carried out. The banned items are listed in our behaviour support policy and procedure, **and/or**

Policy Name: ICT and Internet Acceptable Use Policy	Issue Date: July 2026	Version No: 4
Status: Approved	Next Review Date: July 2027	Page 15 of 38

- Is evidence in relation to an offence

This includes, but is not limited to:

- Pornography
- Abusive messages, images or videos
- Indecent images of children
- Evidence of suspected criminal behaviour (such as threats of violence or assault)

Before a search, if the authorised staff member is satisfied that they have reasonable grounds for suspecting any of the above, they will also:

- Make an assessment of how urgent the search is and consider the risk to other pupils and staff. If the search is not urgent, they will seek advice from the designated safeguarding lead.
- Explain to the pupil why they are being searched, and how and where the search will happen, and give them the opportunity to ask questions about it
- Seek the pupil's co-operation. If the pupil refused to co-operate, we will proceed according to our behaviour support policy and procedure.

The authorised staff member should:

- Inform the DSL (or deputy) of any searching incidents where they had reasonable grounds to suspect a pupil was in possession of a banned item. A list of banned items is available in the behaviour support policy & procedure.
- Involve the DSL (or deputy) without delay if they believe that a search has revealed a safeguarding risk

Authorised staff members may examine, and in exceptional circumstances erase, any data or files on a device that they have confiscated where they believe there is a 'good reason' to do so.

When deciding whether there is a 'good reason' to examine data or files on a device, the staff member should only do so if they reasonably suspect that the data has been, or could be, used to:

- Cause harm, **and/or**
- Undermine the safe environment of the school or disrupt teaching, **and/or**
- Commit an offence

If inappropriate material is found on the device, it is up to Headteacher in conjunction with the DSL to decide on a suitable response. If there are images, data or files on the device that staff reasonably suspect are likely to put a person at risk, they will first consider the appropriate safeguarding response.

When deciding whether there is a good reason to erase data or files from a device, staff members will consider whether the material may constitute evidence relating to a suspected offence. In these instances, they will not delete the material, and the device will be handed to the police as soon as is reasonably practicable. If the material is not suspected to be evidence in relation to an offence, staff members may delete it if:

Policy Name: ICT and Internet Acceptable Use Policy	Issue Date: July 2026	Version No: 4
Status: Approved	Next Review Date: July 2027	Page 16 of 38

- They reasonably suspect that its continued existence is likely to cause harm to any person, **and/or**
- The pupil and/or the parent refuses to delete the material themselves

If a staff member **suspects** a device **may** contain an indecent image of a child (also known as a nude or semi-nude image), they will:

- **Not** view the image
- **Not** copy, print, share, store or save the image
- Confiscate the device and report the incident to the DSL (or deputy) immediately, who will decide what to do next. The DSL will make the decision in line with the DfE's latest guidance on [searching, screening and confiscation](#) and the UK Council for Internet Safety (UKCIS) et al.'s guidance on [sharing nudes and semi-nudes: advice for education settings working with children and young people](#)

Any searching of pupils will be carried out in line with:

- The DfE's latest guidance on [searching, screening and confiscation](#)
- UKCIS et al.'s guidance on [sharing nudes and semi-nudes: advice for education settings working with children and young people](#)
- Our behaviour support policy & procedure / searches and confiscation policy.

Any complaints about searching for, or deleting, inappropriate images or files on pupils' devices will be dealt with through the school complaints procedure.

Unacceptable use of ICT and the internet outside of school

The school will sanction pupils, in line with the behaviour support policy & procedure, if a pupil engages in any of the following **at any time** (even if they are not on school premises):

- Using ICT or the internet to breach intellectual property rights or copyright
- Using ICT or the internet to bully or harass someone else, or to promote unlawful discrimination
- Breaching the school's policies or procedures
- Any illegal conduct, or making statements which are deemed to be advocating illegal activity
- Accessing, creating, storing, linking to or sending material that is pornographic, offensive, obscene or otherwise inappropriate
- Consensual or non-consensual sharing of nude and semi-nude images and/or videos and/or livestreams (also known as sexting or youth produced sexual imagery)
- Activity which defames or disparages the school, or risks bringing the school into disrepute
- Sharing confidential information about the school, other pupils, or other members of the school community
- Gaining or attempting to gain access to restricted areas of the network, or to any password-protected information, without approval from authorised personnel

Policy Name: ICT and Internet Acceptable Use Policy	Issue Date: July 2026	Version No: 4
Status: Approved	Next Review Date: July 2027	Page 17 of 38

- Allowing, encouraging, or enabling others to gain (or attempt to gain) unauthorised access to the school's ICT facilities
- Causing intentional damage to the school's ICT facilities or materials
- Causing a data breach by accessing, modifying, or sharing data (including personal data) to which a user and/or those they share it with are not supposed to have access, or without authorisation
- Using inappropriate or offensive language
- Please see our behaviour support policy and procedure.

Parents/carers

Access to ICT facilities and materials

Parents/carers do not have access to the school's ICT facilities as a matter of course.

However, parents/carers working for, or with, the school in an official capacity (for instance, as a volunteer or as a member of the PTA) may be granted an appropriate level of access or be permitted to use the school's facilities at the headteacher's discretion.

Where parents/carers are granted access in this way, they must abide by this policy as it applies to staff.

Communicating with or about the school online

We believe it is important to model for pupils, and help them learn how to communicate respectfully with, and about, others online.

Parents/carers play a vital role in helping model this behaviour for their children, especially when communicating with the school through our website and social media channels.

We ask parents/carers to sign the agreement in appendix 2.

Communicating with parents/carers about pupil activity

The school will ensure that parents and carers are made aware of any online activity that their children are being asked to carry out.

When we ask pupils to use websites or engage in online activity, we will communicate the details of this to parents/carers in the same way that information about homework tasks is shared.

In particular, staff will let parents/carers know which (if any) person or people from the school pupils will be interacting with online, including the purpose of the interaction.

Parents/carers may seek any support and advice from the school to ensure a safe online environment is established for their child.

Policy Name: ICT and Internet Acceptable Use Policy	Issue Date: July 2026	Version No: 4
Status: Approved	Next Review Date: July 2027	Page 18 of 38

6. Monitoring and Compliance

The Lead DSL, IT Team and Computing DSL monitor the implementation of this policy, including ensuring it is updated to reflect the needs and circumstances of the school.

This policy will be reviewed every year unless a response is required by law.

The governing board is responsible for approving this policy.

7. Associated Policies and References

Relevant legislation and guidance:

This policy refers to, and complies with, the following legislation and guidance:

- [Data Protection Act 2018](#)
- The UK General Data Protection Regulation (UK GDPR) – the EU GDPR was incorporated into UK legislation, with some amendments, by [The Data Protection, Privacy and Electronic Communications \(Amendments etc\) \(EU Exit\) Regulations 2020](#)
- [Computer Misuse Act 1990](#)
- [Human Rights Act 1998](#)
- [The Telecommunications \(Lawful Business Practice\) \(Interception of Communications\) Regulations 2000](#)
- [Education Act 2011](#)
- [Freedom of Information Act 2000](#)
- [Education and Inspections Act 2006](#)
- [Keeping children safe in education 2024 \(publishing.service.gov.uk\)](#)
- [Searching, screening and confiscation: advice for schools 2022](#)
- [National Cyber Security Centre \(NCSC\): Cyber Security for Schools](#)
- [Education and Training \(Welfare of Children\) Act 2021](#)
- UK Council for Internet Safety (et al.) guidance on [sharing nudes and semi-nudes: advice for education settings working with children and young people](#)
- [Meeting digital and technology standards in schools and colleges](#)

This policy should be read alongside the school's policies on:

- Online safety
- Social media
- Safeguarding and child protection

Policy Name: ICT and Internet Acceptable Use Policy	Issue Date: July 2026	Version No: 4
Status: Approved	Next Review Date: July 2027	Page 19 of 38

- Behaviour Support Policy & Procedure
- Staff discipline
- Data protection
- Remote education
- Mobile phone usage
- AI policy
- Bring your own device policy
- Filtering and Monitoring guidelines

Policy Name: ICT and Internet Acceptable Use Policy	Issue Date: July 2026	Version No: 4
Status: Approved	Next Review Date: July 2027	Page 20 of 38

Do not accept friend requests from pupils on social media

10 rules for school staff on Facebook

1. Change your display name – use your first and middle name, use a maiden name, or put your surname backwards instead
2. Change your profile picture to something unidentifiable, or if you don't, make sure that the image is professional
3. Check your privacy settings regularly
4. Be careful about tagging other staff members in images or posts
5. Don't share anything publicly that you wouldn't be happy showing your pupils
6. Don't use social media sites during school hours
7. Don't make comments about your job, your colleagues, our school or your pupils online – once it's out there, it's out there
8. Don't associate yourself with the school on your profile (e.g. by setting it as your workplace, or by 'checking in' at a school event)
9. Don't link your work email address to your social media accounts. Anyone who has this address (or your personal email address/mobile number) is able to find you using this information
10. Consider uninstalling the Facebook app from your phone. The app recognises WiFi connections and makes friend suggestions based on who else uses the same WiFi connection (such as parents or pupils)

Check your privacy settings

- Change the visibility of your posts and photos to **'Friends only'**, rather than 'Friends of friends'. Otherwise, pupils and their families may still be able to read your posts, see things you've shared and look at your pictures if they're friends with anybody on your contacts list
- Don't forget to check your **old posts and photos** – go to bit.ly/2MdQXMN to find out how to limit the visibility of previous posts
- The public may still be able to see posts you've **'liked'**, even if your profile settings are private, because this depends on the privacy settings of the original poster
- **Google your name** to see what information about you is visible to the public

Policy Name: ICT and Internet Acceptable Use Policy	Issue Date: July 2026	Version No: 4
Status: Approved	Next Review Date: July 2027	Page 21 of 38

- Prevent search engines from indexing your profile so that people can't **search for you by name** – go to bit.ly/2zMdVht to find out how to do this
- Remember that **some information is always public**: your display name, profile picture, cover photo, user ID (in the URL for your profile), country, age range and gender

What to do if ...

A pupil adds you on social media

- In the first instance, ignore and delete the request. Block the pupil from viewing your profile
- Check your privacy settings again, and consider changing your display name or profile picture
- If the pupil asks you about the friend request in person, tell them that you're not allowed to accept friend requests from pupils and that if they persist, you'll have to notify senior leadership and/or their parents/carers. If the pupil persists, take a screenshot of their request and any accompanying messages
- Notify the senior leadership team or the headteacher about what's happening

A parent/carer adds you on social media

- It is at your discretion whether to respond. Bear in mind that:
 - Responding to 1 parent/carer's friend request or message might set an unwelcome precedent for both you and other teachers at the school
 - Pupils may then have indirect access through their parent/carer's account to anything you post, share, comment on or are tagged in
- If you wish to decline the offer or ignore the message, consider drafting a stock response to let the parent/carer know that you're doing so

You're being harassed on social media, or somebody is spreading something offensive about you

- **Do not** retaliate or respond in any way
- Save evidence of any abuse by taking screenshots and recording the time and date it occurred
- Report the material to Facebook or the relevant social network and ask them to remove it
- If the perpetrator is a current pupil or staff member, our mediation and disciplinary procedures are usually sufficient to deal with online incidents

Policy Name: ICT and Internet Acceptable Use Policy	Issue Date: July 2026	Version No: 4
Status: Approved	Next Review Date: July 2027	Page 22 of 38

- If the perpetrator is a parent/carer or other external adult, a senior member of staff should invite them to a meeting to address any reasonable concerns or complaints and/or request they remove the offending comments or material
- If the comments are racist, sexist, of a sexual nature or constitute a hate crime, you or a senior leader should consider contacting the police

Policy Name: ICT and Internet Acceptable Use Policy	Issue Date: July 2026	Version No: 4
Status: Approved	Next Review Date: July 2027	Page 23 of 38

Appendix 1: acceptable use agreement (parents/carers)

Adapt this agreement to reflect your school's approach, in line with any changes you made to this policy.

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR PARENTS AND CARERS

Name of pupil:

When I use the school's ICT systems (like computers) and get onto the internet in school I will:

- Ask a teacher or adult if I can do so before using them
- Only use websites that a teacher or adult has told me or allowed me to use
- Tell my teacher immediately if:
 - I click on a website by mistake
 - I receive messages from people I don't know
 - I find anything that may upset or harm me or my friends
- Use school computers for school work only
- Be kind to others and not upset or be rude to them
- Look after the school ICT equipment and tell a teacher straight away if something is broken or not working properly
- Only use the username and password I have been given
- Try my hardest to remember my username and password
- Never share my password with anyone, including my friends
- Never give my personal information (my name, address or telephone numbers) to anyone without the permission of my teacher or parent/carer
- Save my work on the school network
- Check with the class teacher before I print anything
- Log off or shut down a computer when I have finished using it

I agree that the school will monitor the websites I visit and that there will be consequences if I don't follow the rules.

Signed (pupil):

Date:

Parent/carer agreement: I agree that my child can use the school's ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for pupils using the school's ICT systems and internet, and will make sure my child understands these.

Signed (parent/carer):

Date:

Policy Name: ICT and Internet Acceptable Use Policy	Issue Date: July 2026	Version No: 4
Status: Approved	Next Review Date: July 2027	Page 24 of 38

Appendix 2a: Acceptable use agreement for older pupils (Suggested high level AA students)



School policy

Digital technologies have become integral to the lives of children and young people, both within schools and outside school. These technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. Young people should have an entitlement to safe access to these digital technologies.

This acceptable use agreement is intended to ensure:

- that young people will be responsible users and stay safe while using the internet and other digital technologies for educational, personal and recreational use.
- that school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and will have good access to digital technologies to enhance their learning and will, in return, expect the *learners* to agree to be responsible users.

Acceptable Use Agreement - This document is intended to be read by an adult and discussed with each student to ensure their understanding.

I understand that I must use school systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems and other users.

For my own personal safety:

- I understand that the schools will monitor my use of the systems, devices and digital communications.
- I will keep my username and password safe and secure – I will not share it, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it.
- I will be aware of "stranger danger", when I am communicating on-line.
- I will not disclose or share personal information about myself or others when on-line (this could include names, addresses, email addresses, telephone numbers, age, gender, educational details, financial details etc.)
- If I arrange to meet people off-line that I have communicated with on-line, I will do so in a public place and take an adult with me.
- I will immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it on-line.

I understand that everyone has equal rights to use technology as a resource and:

- I understand that the school's systems and devices are primarily intended for educational use and that I will not use them for personal or recreational use unless I have permission.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not use the school's systems or devices for on-line gaming, on-line gambling, internet shopping, file sharing, or video broadcasting (e.g. YouTube), unless I have permission of a member of staff to do so.
- I will not attempt to access, copy, remove or otherwise alter any staff files or documents.

Policy Name: ICT and Internet Acceptable Use Policy	Issue Date: July 2026	Version No: 4
Status: Approved	Next Review Date: July 2027	Page 25 of 38

I will act as I expect others to act toward me:

- I will respect others' work and property and will not access, copy, remove or otherwise alter any other user's files, without the owner's knowledge and permission.
- I will be polite and responsible when I communicate with others, I will not use strong, aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will not take or distribute images of anyone without their permission.

I recognise that the school has a responsibility to maintain the security and integrity of the technology it offers me and to ensure the smooth running of the school:

- I will only use my own personal devices (mobile phones/USB devices etc.) in school if I have permission. I understand that, if I do use my own devices in the school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment.
- If I am using my own personal device, I must be connected to the set PHS network.
- I understand the risks and will not try to upload, download or access any materials which are illegal or inappropriate or may cause harm or distress to others, nor will I try to use any programmes or software that might allow me to bypass the filtering/security systems in place to prevent access to such materials.
- I will immediately report any damage or faults involving equipment or software; however, this may have happened.
- I will not open any hyperlinks in emails or any attachments to emails, unless I know and trust the person/organisation who sent the email, or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes)
- I will not install or attempt to install or store programmes of any type on any school device, nor will I try to alter computer settings.
- I will only use social media sites with permission and at the times that are allowed.

When using the internet for research or recreation, I recognise that:

- I should ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not try to download copies (including music and videos)
- When I am using the internet to find information, I should take care to check that the information that I access is accurate, as I understand that the work of others may not be truthful and may be a deliberate attempt to mislead me.
- I should not use AI tools and generative chatbots (such as ChatGPT and Google Bard) during assessments, including internal and external assessments, and coursework, or to write my homework or class assignments, where AI-generated text or imagery is presented as my own work.
- I should only use approved AI tools (CoPilot).

I understand that I am responsible for my actions, both in and out of school:

- I understand that the school also has the right to take action against me if I am involved in incidents of inappropriate behaviour, that are covered in this agreement, when I am out of school and where they involve my membership of the school community (examples would be online-bullying, use of images or personal information).
- I understand that if I fail to comply with this acceptable use agreement, I may be subject to disciplinary action. This could include loss of access to the school network/internet, detentions, suspensions, contact with parents and in the event of illegal activities involvement of the police.

Please complete the sections on the next page to show that you have read, understood and agree to the rules included in the acceptable use agreement. If you do not sign and return this agreement, access will not be granted to school systems and devices.

Learner Acceptable Use Agreement Form

Policy Name: ICT and Internet Acceptable Use Policy	Issue Date: July 2026	Version No: 4
Status: Approved	Next Review Date: July 2027	Page 26 of 38

This form relates to the learner acceptable use agreement; to which it is attached.

Please complete the sections below to show that you have read, understood and agree to the rules included in the acceptable use agreement. If you do not sign and return this agreement, access will not be granted to school systems. (Schools will need to decide if they require learners to sign, or whether they wish to simply make them aware through education programmes/awareness raising).

I have read and understand the above and agree to follow these guidelines when:

- I use the school's systems and devices (both in and out of school)
- I use my own devices in the school (when allowed) e.g. mobile phones, gaming devices USB devices, cameras etc.
- I use my own equipment out of the school in a way that is related to me being a member of this school e.g. communicating with other members of the school, accessing school email, VLE, website etc.

Name of Learner:

Group/Class:

Signed:

Date:

Copyright of these policy templates is held by SWGfL. Schools/colleges and other educational institutions are permitted free use of the policy templates for the purposes of policy review and development. Any person or organisation wishing to use the document for other purposes should seek consent from SWGfL (onlinesafety@swgfl.org.uk) and acknowledge its use.
© SWGfL 2022

Policy Name: ICT and Internet Acceptable Use Policy	Issue Date: July 2026	Version No: 4
Status: Approved	Next Review Date: July 2027	Page 27 of 38

Appendix 2b1: Acceptable use agreement for younger pupils (suggested KS4+)

Introduction - This document is intended to be read by an adult and discussed with each student to ensure their understanding.

Digital technologies have become integral to the lives of children and young people, both within and outside schools. These technologies are powerful tools, which open-up new opportunities for everyone. They can stimulate discussion, encourage creativity and stimulate awareness of context to promote effective learning. Learners should have an entitlement to safe access to these digital technologies.

This acceptable use agreement is intended:

- to ensure that learners will have good access to devices and online content, be responsible users and stay safe while using digital technologies for educational, personal and recreational use
- to help learners understand good online behaviours that they can use in school, but also outside school
- to protect school devices and networks from accidental or deliberate misuse that could put the security of the systems and users at risk.

Acceptable Use Agreement

When I use devices I must behave responsibly to help keep me and other users safe online and to look after the devices.

For my own personal safety:

- I understand that what I do online will be supervised and monitored and that I may not be allowed to use devices in school unless I follow these rules and use them responsibly
- I will only visit internet sites that adults have told me are safe to visit
- I will keep my username and password safe and secure and not share it with anyone else
- I will be aware of “stranger danger” when I am online
- I will not share personal information about myself or others when online
- If I arrange to meet people off-line that I have communicated with online, I will do so in a public place and take a trusted adult with me
- I will immediately tell an adult if I see anything that makes me feel uncomfortable when I see it online.

I will look after the devices I use, so that the school and everyone there can be safe:

- I will handle all the devices carefully and only use them if I have permission.
- I will not try to alter the settings on any devices or try to install any software or programmes.
- I will tell an adult if a device is damaged or if anything else goes wrong.
- I will only use the devices to do things that I am allowed to do.

I will think about how my behaviour online might affect other people:

- When online, I will act as I expect others to act toward me.
- I will not copy anyone else’s work or files without their permission.
- I will be polite and responsible when I communicate with others and I appreciate that others may have different opinions to me.
- I will not take or share images of anyone without their permission.

I know that there are other rules that I need to follow:

- I will only use my own personal devices (mobile phones/USB devices etc.) in the school if I have permission. If I am allowed, I still have to follow all the other school rules if I use them.

Policy Name: ICT and Internet Acceptable Use Policy	Issue Date: July 2026	Version No: 4
Status: Approved	Next Review Date: July 2027	Page 28 of 38

- If I am using my own personal device, I must be connected to the set PHS network.
- I will only use social media sites with permission and at the times that are allowed.
- Where work is protected by copyright, I will not try to download copies (including music and videos).
- When I am using the internet to find information, I should take care to check that the information is accurate, as I understand that the work of others may not be truthful and may be a deliberate attempt to mislead me.
- I should have permission if I use the original work of others in my own work.
- I should not use AI tools and generative chatbots (such as ChatGPT and Google Bard) to complete any of my class assignments or homework.
- I should only use approved AI tools (CoPilot).

I understand that I am responsible for my actions, both in and out of school:

- I know that I am expected to follow these rules in school and that I should behave in the same way when out of school as well.
- I understand that if I do not follow these rules, I may be subject to disciplinary action. This could include loss of access to the school network/internet, detentions, suspensions, parents/carers contacted and in the event of illegal activities involvement of the police.

Learner Acceptable Use Agreement Form

Please complete the sections below to show that you have read, understood and agree to the rules included in the acceptable use agreement. If you do not sign and return this agreement, access will not be granted to school systems. I have read and understand the above and agree to follow these guidelines when:

- I use the school systems and devices (both in and out of school)
- I use my own devices in the school (when allowed) e.g. mobile phones, gaming devices USB devices, cameras etc.
- I am out of school and involved in any online behaviour that might affect the school or other members of the school.

Copyright of these policy templates is held by SWGfL. Schools/colleges and other educational institutions are permitted free use of the policy templates for the purposes of policy review and development. Any person or organisation wishing to use the document for other purposes should seek consent from SWGfL (onlinesafety@swgfl.org.uk) and acknowledge its use.
© SWGfL 2022.

Policy Name: ICT and Internet Acceptable Use Policy	Issue Date: July 2026	Version No: 4
Status: Approved	Next Review Date: July 2027	Page 29 of 38

Appendix 2b2- User agreement

- 1. For my own personal safety, I understand that what I do online will be supervised and monitored and that I may not be allowed to use devices in school unless I follow these rules.**
- 2. I will look after the devices that I use so that the school and everyone there can be safe.**
- 3. I will think about how my behaviour online might affect other people.**
- 4. If I am using my own personal device, I must stay connected to a PHS network and follow the same rules for school devices.**
- 5. I understand that I am responsible for my actions, both in and out of school.**
- 6. I understand that if I do not follow these rules, I may be restricted in my use or not be able to use technology at all in school.**

Name of Learner:

Signed:

Class group:

Date:

Policy Name: ICT and Internet Acceptable Use Policy	Issue Date: July 2026	Version No: 4
Status: Approved	Next Review Date: July 2027	Page 30 of 38

Appendix 2c: Acceptable use agreement for younger pupils (1, suggested EYFS, KS1, KS2, KS3 and Nurture students).





Computer Agreement

1. I will ask an adult if I want to use any

technology.

2. I will only use activities that I have been told

to use by an adult.

3. I will take care of the technology.

4. I will ask for help from an adult if I am not

sure what to do or if I think I have done

something wrong.

Policy Name: ICT and Internet Acceptable Use Policy	Issue Date: July 2026	Version No: 4
Status: Approved	Next Review Date: July 2027	Page 31 of 38

5. I will tell an adult if I see something that

upsets me on a screen.

6. I know that if I break the rules I might not be

allowed to use technology.

Signed (my name) _____

Policy Name: ICT and Internet Acceptable Use Policy	Issue Date: July 2026	Version No: 4
Status: Approved	Next Review Date: July 2027	Page 32 of 38

Appendix 3: Acceptable use agreement for staff, governors, volunteers and visitors



School Policy

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school. The internet and other digital information and communications technologies are powerful tools, which open new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. They also bring opportunities for staff to be more creative and productive in their work. All users should have an entitlement to safe access to the internet and digital technologies at all times.

This acceptable use policy is intended to ensure:

- that staff and volunteers will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- that school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that staff are protected from potential risk in their use of technology in their everyday work.

The school will try to ensure that staff and volunteers will have good access to digital technology to enhance their work, to enhance learning opportunities for learning and will, in return, expect staff and volunteers to agree to be responsible users.

Acceptable Use Policy Agreement

I understand that I must use school systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems and other users. I recognise the value of the use of digital technology for enhancing learning and will ensure that learners receive opportunities to gain from the use of digital technology. I will, where possible, educate the young people in my care in the safe use of digital technology and embed online safety in my work with young people.

For my professional and personal safety:

- I understand that the school will monitor my use of the school digital technology and communications systems.
- I understand that the rules set out in this agreement also apply to use of these technologies (e.g., laptops, email, VLE etc.) out of school, and to the transfer of personal data (digital or paper based) out of school
- I understand that the school digital technology systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by the school.
- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it.
- I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.

I will be professional in my communications and actions when using school systems:

Policy Name: ICT and Internet Acceptable Use Policy	Issue Date: July 2026	Version No: 4
Status: Approved	Next Review Date: July 2027	Page 33 of 38

- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
- I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will ensure that when I take and/or publish images of others I will do so with their permission and in accordance with the school's policy on the use of digital/video images. I will not use my personal equipment to record these images, unless I have permission to do so. Where these images are published (e.g., on the school website/VLE) it will not be possible to identify by name, or other personal information, those who are featured.
- I will only use social networking sites in school in accordance with the school's policies.
- I will only communicate with learners and parents/carers using official school systems. Any such communication will be professional in tone and manner.
- I will not engage in any on-line activity that may compromise my professional responsibilities.
- I will only use approved AI tools (CoPilot).

The school has the responsibility to provide safe and secure access to technologies and ensure the smooth running of the school:

- When I use my mobile devices in school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment. I will also follow any additional rules set by the school about such use. I will ensure that any such devices are protected by up-to-date anti-virus software and are free from viruses.
- I will not use personal email addresses on the school's ICT systems.
- I will not open any hyperlinks in emails or any attachments to emails, unless the source is known and trusted, or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes)
- I will ensure that my data is regularly backed up, in accordance with relevant school policies.
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, terrorist or extremist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering/security systems in place to prevent access to such materials.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings, unless this is allowed in school policies.
- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- I will only transport, hold, disclose or share personal information about myself or others, as outlined in the School Personal Data Policy (or other relevant policy). Where digital personal data is transferred outside the secure local network, it must be encrypted. Paper based documents containing personal data must be held in lockable storage.
- I understand that data protection policy requires that any staff or learner data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by school policy to disclose such information to an appropriate authority.
- I will immediately report any damage or faults involving equipment or software; however this may have happened.

Policy Name: ICT and Internet Acceptable Use Policy	Issue Date: July 2026	Version No: 4
Status: Approved	Next Review Date: July 2027	Page 34 of 38

When using the online systems in my professional capacity or for school sanctioned personal use:

- I will ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not download or distribute copies (including music and videos).

I understand that I am responsible for my actions in and out of the school:

- I understand that this acceptable use policy applies not only to my work and use of school's digital technology equipment in school, but also applies to my use of school systems and equipment off the premises and my use of personal equipment on the premises or in situations related to my employment by the school
- I understand that if I fail to comply with this acceptable use agreement, I could be subject to disciplinary action. This could include a warning, a suspension, referral to Governors/Trustees and/or the Local Authority and in the event of illegal activities the involvement of the police.

I have read and understand the above and agree to use the school digital technology systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.

Staff/Volunteer Name:

Signed:

Date:

Copyright of these policy templates is held by SWGfL. Schools/colleges and other educational institutions are permitted free use of the policy templates for the purposes of policy review and development. Any person or organisation wishing to use the document for other purposes should seek consent from SWGfL (onlinesafety@swgfl.org.uk) and acknowledge its use.

Appendix 6: 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.
Breach	When your data, systems or networks are accessed or changed in a non-authorised way.
Cloud	Where you can store and access your resources

Policy Name: ICT and Internet Acceptable Use Policy	Issue Date: July 2026	Version No: 4
Status: Approved	Next Review Date: July 2027	Page 35 of 38

TERM	DEFINITION
	(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.
Pharming	An attack on your computer network that means

Policy Name: ICT and Internet Acceptable Use Policy	Issue Date: July 2026	Version No: 4
Status: Approved	Next Review Date: July 2027	Page 36 of 38

TERM	DEFINITION
	users are redirected to a wrong or illegitimate website even if they type in the right website address.
Phishing	Untargeted, mass emails sent to many people asking for sensitive information (such as 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.
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	Programmes 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

Policy Name: ICT and Internet Acceptable Use Policy	Issue Date: July 2026	Version No: 4
Status: Approved	Next Review Date: July 2027	Page 37 of 38

TERM	DEFINITION
	are made to look legitimate) aimed at senior people in an organisation.

Policy Name: ICT and Internet Acceptable Use Policy	Issue Date: July 2026	Version No: 4
Status: Approved	Next Review Date: July 2027	Page 38 of 38