



ICT and internet acceptable use Policy

Introduction and aims.

Information and communications technology (ICT) is an integral part of the way our school functions, and is a critical resource for pupils, staff (including senior leadership teams), governors, volunteers, and visitors. It supports teaching and learning, pastoral and administrative functions of the school. However, the ICT resources and facilities our school uses also pose risks to data protection, online safety and safeguarding.

This policy aims to:

- Set guidelines and rules on the use of school ICT resources for staff, pupils, parents and governors
- Establish clear expectations for the way all members of the school community engage with each other online
- Support the school's policy on GDPR, data protection, online safety and safeguarding
- Prevent disruption 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 policy, Volunteers in school policy, Staff and Governor codes of conduct.

This policy should be read in conjunction with the School's Online Safety Policy.

Relevant legislation and guidance

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

- [Data Protection Act 2018](#)
- [The General Data Protection Regulation](#)
- [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](#)
- [The Education and Inspections Act 2006](#)
- [Keeping Children Safe in Education 2021](#)
- [Searching, screening and confiscation: advice for schools](#)
- [National Cyber Security Centre \(NCSC\)](#)
- [Education and Training \(Welfare of Children Act\) 2021](#)

Definitions

- **"ICT facilities"**: includes 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 which may become available in the future which is provided as part of the ICT service

Written	Ratified	Review
November 2022	HT	3 Years

- **“Users”**: anyone authorised by the school to use the 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
- **“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 ICT facilities including but not limited to documents, photos, audio, video, printed output, web pages, social networking sites and blogs

Unacceptable use

The following is considered unacceptable use of the school’s ICT facilities by any member of the school community. 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
- Consensual and 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, 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 program, tool or item of software designed to interfere with the functioning of the 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 ICT facilities
- Removing, deleting or disposing of ICT equipment, systems, programs or information without permission by authorised personnel
- Causing a data breach by accessing, modifying, or sharing data (including personal data) to which a user is not supposed 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 mechanisms
- Engaging in content or conduct that is radicalised, extremist, racist, anti-Semitic or discriminatory in any other way

This is not an exhaustive list. The school reserves the right to amend this list at any time. The members of the Senior Leadership Teams will use professional judgement to determine whether any act or behaviour not on the list above is considered unacceptable use of the school’s ICT facilities.

Sanctions

Pupils and staff who engage in any of the unacceptable activity listed above may face disciplinary action in line with the school’s policies

Written	Ratified	Review
November 2022	HT	3 Years

Staff (including governors, volunteers, and contractors)

[Access to school ICT facilities and materials](#)

The school's network manager ICT Network Services manages access to the school's ICT facilities and materials for school staff. This includes, but is not limited to:

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

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

Staff who have access to files they are not authorised to view or edit, or who need their access permissions updated or changed, should contact the network manager, SLT or SBM.

All equipment accessing to the school's internet is required to have an individual and traceable IP address linked to approved users. Use of the school's network is monitored, and inappropriate activities reported to the Network Manager and the Headteacher.

Ad hoc access is made available to the school's Guest network to enable visitors on site internet access. This system is password protected.

[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. All work-related business should be conducted using the email address the school has provided. Communications with Families should be via Arbor or forwarded by the School Office. The school seeks to limit the number of email communications with families and where possible information must be disseminated in the weekly newsletter.

Staff must not share their personal email addresses with parents 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.

Staff must take extra care when sending sensitive or confidential information by email to external third parties. 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 a member of SLT immediately and follow the school's data breach procedure, by reporting a GDPR Breach using the GDPRiS platform.

Staff must not give their personal phone numbers to parents 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.

[Subject Access Requests](#)

Written	Ratified	Review
November 2022	HT	3 Years

Email messages are required to be disclosed in legal proceedings or in response to Subject Access Requests (SARs) 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.
- Emails concerning pupils/colleagues/families must be professional and contain only content you would be comfortable with the family reading.
- Records where a pupil is referred to by initials are also required to be disclosed in a SAR.
- Emails referring to several individuals will require all other names to be redacted before inclusion in a SAR and consideration needs to be given to the appropriateness of grouping pupils in one email.

Personal use

Staff are permitted to occasionally use school ICT facilities for personal use subject to certain conditions set out below. Personal use of ICT facilities must not be overused or abused. The SLT may withdraw permission for it at any time or restrict access at their discretion.

Personal use is permitted provided that such use:

- Does not take place during contact time/teaching hours/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

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 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 could see them.

Staff should take care to follow the school's guidelines on social media (see appendix 1) and use of email to protect themselves online and avoid compromising their professional integrity.

Personal social media accounts

Members of staff should ensure 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 using Office 365. 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 equipment and facilities outside the school and take such precautions 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 Twitter page, managed by the headteacher. Staff members who have not been authorised to manage, or post to, the account, must not access, or attempt to access the account.

Monitoring of school network and use of ICT facilities

Written	Ratified	Review
November 2022	HT	3 Years

The school reserves the right to monitor the use of its ICT facilities and network. This includes, but is not limited to, monitoring of:

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

Only authorised ICT staff may inspect, monitor, intercept, assess, record and disclose the above, to the extent permitted by law.

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
- Prevent or detect crime
- Comply with a subject access request, Freedom of Information Act request, or any other legal obligation

Pupils

Please refer to Online Safety and Child protection Policies

Parents

Access to ICT facilities and materials

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

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

Where parents 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 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.

Data security

The school is responsible for making sure it has the appropriate level of security protection and procedures in place. It therefore takes steps to protect the security of its computing resources, data and user accounts. However, the school cannot guarantee security. Staff, pupils, parents and others who use the school's ICT facilities should use safe computing practices at all times.

Passwords

All users of the school's ICT facilities should set strong passwords for their accounts 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. Double Authentication is enabled to gain access the school's 365 Account.

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

Written	Ratified	Review
November 2022	HT	3 Years

All staff will use a password manager to help them store their passwords securely. Teachers will generate passwords for pupils using a password manager/generator and keep these in a secure location in case pupils lose or forget their passwords.

Written	Ratified	Review
November 2022	HT	3 Years

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 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.

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.

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 a member of SLT 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 closed down completely at the end of each working day.

Encryption

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

School staff may only use personal devices - including computers - to access school data, work remotely, or take personal data (such as pupil information) out of school if they have been specifically authorised to do so by the headteacher. Personal data accessed remotely on Office 365 may not be downloaded to personal devices.

Use of such personal devices will only be authorised if the devices have appropriate levels of security and encryption, as defined by the ICT Manager.

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 manager to make sure cyber security is given the time and resources it needs to make the school secure
- 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
- Back up critical data daily and store these backups on cloud based backup systems
- Delegate specific responsibility for maintaining the security of our management information system (MIS) to our ICT Manager
- Make sure ICT staff conduct regular access reviews to make sure each user in the school has the right level of permissions and admin rights
- Have a firewall in place that is switched on
- Develop, review and test an incident response plan with the IT department, for example, including how the school will communicate with everyone if communications go down, who will be contacted when, and who will notify.

Written	Ratified	Review
November 2022	HT	3 Years

Internet access

The school wireless internet connection is secured and the LEA Filtering system, Smoothwall, is used for all devices accessing the connection.

Parents and visitors

Parents and visitors to the school will not be permitted to use the school's Guest Wi-Fi unless specific authorisation is granted by the headteacher.

The headteacher will only grant authorisation if:

Parents are working with the school in an official capacity (e.g. as a volunteer or as a member of the PTA)

Governors and other Visitors need to access the school's Wi-Fi 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)

Staff must not give the Wi-Fi password to anyone who is not authorised to have it. Doing so could result in disciplinary action.

Related policies

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

- Online safety
- Safeguarding and child protection
- Behaviour
- Staff discipline
- Code of Conduct
- Data protection
- Remote learning
- Mobile phone usage

Written	Ratified	Review
November 2022	HT	3 Years

Appendix 1: Facebook cheat sheet for staff

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 not, ensure 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 just as 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 Wi-Fi connections and makes friend suggestions based on who else uses the same Wi-Fi connection (such as parents or pupils)

Never accept friend requests from pupils on social media

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
- 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. 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

Written	Ratified	Review
November 2022	HT	3 Years

A parent adds you on social media

It is at your discretion whether to respond. Bear in mind that:

- Responding to one parent'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'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 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
- If the perpetrator is a parent 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

Written	Ratified	Review
November 2022	HT	3 Years

Appendix 5: Acceptable use agreement for staff, governors, volunteers and visitors

Acceptable use of the school's ICT facilities and the internet: agreement for staff, governors, volunteers and visitors

Name of staff member/governor/volunteer/visitor:

When using the school's ICT facilities and accessing the internet in school, or outside school on a work device, I will not:

- Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature (or create, share, link to or send such material)
- Use them in any way which could harm the school's reputation
- Access social networking sites or chat rooms
- Use any improper language when communicating online, including in emails or other messaging services
- Install any unauthorised software, or connect unauthorised hardware or devices to the school's network
- Share my password with others or log in to the school's network using someone else's details
- Share confidential information about the school, its pupils or staff, or other members of the community
- Access, modify or share data I'm not authorised to access, modify or share
- Promote private businesses, unless that business is directly related to the school

- I understand that the school will monitor the websites I visit and my use of the school's ICT facilities and systems including Wi-Fi.
- I will take all reasonable steps to ensure that work devices are secure and password-protected when using them outside school, and keep all data securely stored in accordance with this policy and the school's data protection policy.
- I will let the designated safeguarding lead (DSL) and ICT manager know if a pupil informs me, they have found any material which might upset, distress or harm them or others, and will also do so if I encounter any such material.
- I will always use the school's ICT systems and internet responsibly and ensure that pupils in my care do so too.

I understand that: -

- the General Data Protection Regulation (GDPR) apply to all personal data held in school, this includes Pupils, Staff, Governors, families, Volunteers and Contractors
- if I fail to adhere to the requirements of the Data Management Policy it is my responsibility to self-report if a breach occurs.
- I may become personally liable for any fines levied by the ICO or compensation claimed by injured parties as a result of my actions where I have not complied with the School's Policies.
- the Acceptable Use Policy Agreement applies not only to my work and use of School 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
- if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action. This could include a warning, a suspension or referral to Governors and, in the event of illegal activities, the involvement of the police.

Signed (staff member/governor/volunteer/visitor):

Date:

Written	Ratified	Review
November 2022	HT	3 Years

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.
Spear-phishing	A more targeted form of phishing where an email is designed to look like it's from a person the recipient

Written	Ratified	Review
November 2022	HT	3 Years

TERM	DEFINITION
	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.

Written	Ratified	Review
November 2022	HT	3 Years