



We can and we will'
GLEBE PRIMARY SCHOOL

ICT and Acceptable Use Policy and Agreement

Introduction and aims

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 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, visitors, and anyone who has access to our IT and communication systems.

Misuse of IT and communications systems can damage our school and our reputation. Breaches of this policy may be dealt with under the disciplinary policy.

Relevant legislation and guidance

This policy refers to, complies with, or otherwise has regard to, 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](#)
- [Data \(Use and Access\) Act 2025](#)
- [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 2025](#)
- › [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](#)
- › [Meeting digital and technology standards in schools and colleges](#)

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 4 for a glossary of cyber security terminology.

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 any web page or downloading any image, document, application, or file from the internet which could be regarded as illegal, offensive, discriminatory, in bad taste, or immoral
- › 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
- › 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

- Using the school's systems to participate in internet chat rooms, post on internet message boards or blogs, unless approved by authorised personnel
- 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 internet and 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

This is not an exhaustive list. The school reserves the right to amend this list at any time.

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.

Staff (including governors, volunteers and contractors)

Access to school ICT facilities and materials

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

- Computers, tablets 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 ICT Inspire.

Use of school-supplied equipment

School-issued devices (including laptops, tablets and other digital devices) are provided to staff for the purpose of supporting teaching, learning and the efficient running of the school. All school-supplied equipment remains the property of the school and staff must return the equipment at the end of employment, or when it is no longer required.

Staff must:

- Use equipment and devices for school purposes and in line with the school's policies on safeguarding, data protection and confidentiality
- Store devices securely when not in use, particularly when travelling. Devices should not be left unattended in public places or in unsecured locations
- Be actively aware of data security and confidentiality and follow best practice when accessing the equipment away from school. E.g. when travelling on public transport, be aware that other passengers may be able to read any documents displayed on the screen of your device
- Lock devices with a password when unattended. Passwords must:
 - Not be shared with others and must be changed regularly
 - Be suitably strong
 - Not be reused across multiple accounts
- Update software, operating systems and applications when prompted, or as directed by ICT Inspire
- Connect to the school network using approved and secure methods. When connecting to wi-fi networks outside of the school, staff must ensure connections are secure and avoid transmitting sensitive data over public or unsecured networks
- Report any loss, theft, damage or compromise of a school device promptly to ICT Inspire and designated safeguarding lead and data protection officer

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.

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.

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 ICT Inspire immediately and follow our data breach procedure.

Staff must not give their personal phone number(s) to parents/carers or pupils. In circumstances where staff are provided with phones, these staff must use the 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.

The school can record incoming and outgoing phone conversations.

Personal use

Staff may not use the school's ICT facilities to store personal, non-work-related information or materials (such as music, videos, personal documentation 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 may not store any school-related data on personal devices, on cloud storage or on personal removable storage devices.

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.

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 social media use in the school's E-safety policy.

Remote access

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

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.

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.

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

To comply with Department for Education (DfE) guidance on [meeting digital and technology standards](#), and 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
- Telephone calls
- 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.

The school reserves the right to retrieve the contents of email messages or to check internet usage (including pages visited and searches made) as reasonably necessary in the interests of the school, including for the following purposes:

- To monitor whether the use of the email system or the internet is legitimate and in accordance with this policy

- To find lost messages or retrieve messages lost due to computer failure
- To help in the investigation of alleged wrongdoing
- To comply with any legal obligation

The list above is not exhaustive.

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

Pupils

Access to ICT facilities

- Computers and equipment in the school's ICT suite are available to pupils only under the supervision of staff
- Logins and passwords are provided to pupils, for educational purposes only. Pupils must not share their passwords with others, or use their accounts to share or download files, including software from the Internet or inappropriate content.
- Specialist ICT equipment, such as that used for music, or design and technology, must only be used under the supervision of staff

Unacceptable use of ICT and the internet outside of school

The school will sanction pupils 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
- 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

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 cyber crime 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

8.1 Passwords

All users of the school's ICT facilities should set strong passwords for their accounts and keep these passwords secure. Users must not use the same passwords across multiple platforms.

Users are responsible for the security of their passwords and accounts, and for setting permissions for accounts and files they control. You must keep these passwords confidential and change them regularly.

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 should not delete, destroy or modify existing systems, programs, information or data. Users must not download or install software from external sources.

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 incoming files should always be virus-checked by ICT Inspire before they are downloaded.

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.

These access rights are managed by ICT Inspire.

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 headteacher 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 only use personal devices (including computers and USB drives) 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.

Use of such personal devices will only be authorised if the devices have appropriate levels of security and encryption.

10.2 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 headteacher.

The headteacher will only grant authorisation if:

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

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

Reviewed: October 2026

To be reviewed: October 2027

Appendix 1: Acceptable use agreement for older pupils

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

Name of pupil: _____

I will read and follow the rules in the Acceptable Use Policy.	When I use the school's ICT systems (including computers, tablets and other devices) and access the internet, I will: • Always use the school's ICT systems and the internet responsibly and for educational purposes only. • Only use them when a teacher is present, or with a teacher's permission. • Keep my username and password safe and not share these with others. • Keep my private information safe at all times and not give my name, address or telephone number to anyone without the permission of my teacher or parent/carer. • Tell a teacher (or sensible adult) immediately if I find any material which might upset, distress or harm me or others. • Use appropriate and respectful language when communicating online. • Always log off or shut down a computer or device when I am finished using it.
I will not:	• Use the school's ICT systems for non-educational purposes unless authorised by a member of staff. • Use ICT facilities to break school rules. • Access any inappropriate websites or content. • Access social networking sites, chat rooms and gaming sites unless my teacher has expressly allowed this as part of a learning activity. • Open any attachments in emails, or follow any links in emails, without first checking with a teacher. • Use any inappropriate language when communicating online, including in emails. • Share images, videos or livestreams of others using school ICT systems. • Log in to the school's network using someone else's details. • Share my password with others. • Bully, harass or intimidate other people online. • Arrange to meet anyone offline without first consulting my parent/carer, or without adult supervision.
If I bring a personal mobile phone or other personal electronic device into school:	• I will not use it during lessons, tutor group time, clubs or other activities organised by the school, without a teacher's permission. • I will use it responsibly, and will not access any inappropriate websites, content or materials, or use inappropriate language when communicating online.
I understand that:	• The school will monitor the websites I visit and my use of the school's ICT facilities and systems. • I must immediately report any material or behaviour online that may upset, distress or harm me or others. • There will be consequences if I do not follow these rules. • The school may discipline me for certain unacceptable online behaviours, even when I am not in school.
I agree to use the school's ICT systems and internet responsibly at all times.	
Signed (pupil):	
Date:	
Parent/carer's 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 for using personal electronic devices in school, and will make sure my child understands these expectations and follows them.
Signed (parent/carer):	
Date:	

Appendix 2: Acceptable use agreement for younger pupils

ACCEPTABLE USE OF THE SCHOOL'S ICT FACILITIES AND INTERNET: AGREEMENT FOR PUPILS AND PARENTS/CARERS - KS1

Name of pupil: _____

When I use the school's ICT systems and facilities (such as computers, tablets and other equipment) and access the internet in school, I will:	• Ask a teacher or adult for permission before using them. • Only use websites and online resources that a teacher or adult has allowed me to use. • Use school computers and equipment for schoolwork and learning activities only. • Be kind and respectful to others when using technology. • Look after 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 best to remember my username and password and keep them safe. • Never give my personal information (such as my name, address or telephone number) to anyone without permission from my teacher or parent/carer. • Save my work on the school network where appropriate. • Check with my teacher before printing anything. • Log off or shut down a computer or device when I have finished using it. • Tell a teacher or trusted member of staff immediately if I find anything online that upsets me, may harm me or others, or if I receive messages from people I do not know.
I will not:	• Use the school's ICT systems or facilities without permission from a teacher or responsible adult. • Use them to break school rules. • Access inappropriate websites or online content. • Access social networking sites unless directly permitted by a teacher for a learning activity. • Use chat rooms. • Open email attachments or click on email links without checking with a teacher first. • Use unkind, rude or inappropriate language when communicating online or by email. • Send or share photos, videos or livestreams of myself or others. • Share my password with anyone else or log in using someone else's username or password. • Bully, harass or upset other people online.
I understand that:	• The school will monitor the websites I visit and how I use the school's ICT systems and equipment to help keep me safe and ensure I follow the rules. • I must tell a teacher or member of staff immediately if I find anything online that is upsetting, harmful, inappropriate or wrong. • I must always use the school's ICT systems and internet responsibly. • There will be consequences if I do not follow these rules. • The school may discipline me if I do certain unacceptable things online, even when I am not in school.
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 and follows these rules.
Signed (parent/carer):	_____
Date:	_____

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

ACCEPTABLE USE OF THE SCHOOL'S ICT FACILITIES AND INTERNET: AGREEMENT FOR STAFF, GOVERNORS, VOLUNTEERS AND VISITORS

Name of staff member/governor/
volunteer/visitor: _____

When using the school's ICT facilities and systems and accessing the internet in school, or outside school on a work device (if applicable), I will:

- Only use the school's ICT systems and internet for educational purposes or for fulfilling the duties of my role.
- Take all reasonable steps to ensure that work devices are secure, password-protected and used in accordance with the school's data protection requirements.
- Keep all data securely stored in line with this policy and the school's data protection policy.
- Report any material that may upset, distress or harm pupils or others to the Designated Safeguarding Lead (DSL) and ICT Manager.
- Ensure that pupils in my care use the school's ICT systems and internet responsibly and safely.

I will not:

- Access, or attempt to access, any illegal, unauthorised, inappropriate or harmful material.
- Use the school's ICT systems in any way that could damage the school's reputation.
- Access social networking sites or chat rooms unless authorised for a legitimate school purpose.
- Use improper, offensive or inappropriate language when communicating online, including by email or other messaging services.
- Install 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 another person's credentials.
- Take photographs of pupils without prior authorisation from the appropriate member of staff and in accordance with school procedures.
- Share confidential information about the school, its pupils, staff or other members of the school community.
- Access, modify, copy or share data that I am not authorised to access, modify or share.
- Promote any private business or commercial activity unless it is directly related to the school's work.

I understand that:

- The school will monitor the websites I visit and my use of the school's ICT facilities, systems and internet access.
- I am responsible for ensuring that all school data remains secure when working on or off site.
- I must notify the DSL and ICT Manager if a pupil reports finding material that may upset, distress or harm themselves or others, or if I encounter such material myself.
- Failure to comply with this agreement may result in disciplinary action and/or withdrawal of access to school ICT systems.

I agree to use the school's ICT systems and internet responsibly, professionally and in accordance with all school policies at all times.

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

Date: _____

TERM	DEFINITION
	which includes viruses, trojans or any code or content that is harmful.
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 with the end aim of fixing them.
Pharming	An attack on your computer network that means users are redirected to a wrong or illegitimate website even if they type in the right website address.
Phishing	Untargeted, mass emails or text messages sent to many people asking for sensitive information (such as bank details or passwords) or encouraging them to visit a fake website.
Ransomware	Malicious software that stops you from using your data or systems, usually by encrypting your files, until you make a payment (a ransom) for decryption.
Social engineering	Manipulating people into giving information or carrying out specific actions that's of use to an attacker.
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.

TERM	DEFINITION
Whaling	Highly-targeted phishing attacks (where emails are made to look legitimate) aimed at senior people in an organisation.