ICT and Internet Acceptable Use Policy

Last Review:	March 2026
Committee:	Curriculum Committee
Date Ratified:	March 2026

Contents

1. Introduction and aims

Information and communications technology (ICT) is an integral part of the way our school works, and is a critical resource for students, 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, students, 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 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 students safe and effective internet and ICT use

Safeguarding and online safety considerations arising from the use of ICT and internet technologies are addressed through the school's Online Safety Policy and Safeguarding and Child Protection Policy. This policy should therefore be read alongside those documents.

This policy applies to all users of the school's ICT facilities, including staff, students, governors, volunteers, contractors and visitors.

Breaches of this policy may result in action being taken in line with the relevant school policies, including the Behaviour Policy, Staff Code of Conduct and disciplinary procedures.

2. Relevant legislation and guidance

This policy should be read in conjunction with the school's Online Safety Policy, which sets out the school's safeguarding responsibilities and procedures in relation to online safety.

This policy reflects, and complies with, the following legislation and statutory guidance (as updated from time to time):

- 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 (latest version)
- Searching, screening and confiscation: advice for schools
- Online Safety Act 2023
- National Cyber Security Centre (NCSC)
- Education and Training (Welfare of Children Act) 2021

Detailed safeguarding expectations, roles and procedures relating to online safety are set out in the school's Online Safety Policy and Safeguarding and Child Protection Policy.

3. 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
- **"Users":** anyone authorised by the school to use the ICT facilities, including governors, staff, students, 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

4. 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).

Safeguarding concerns arising from unacceptable ICT use are managed in accordance with the school's Online Safety Policy and Safeguarding and Child Protection Policy.

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
- Creating, sharing or storing nude or semi-nude images or videos of any person.
- Activity which defames or disparages the school, or risks bringing the school into disrepute
- Sharing confidential information about the school, its students, 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
- Accessing, creating or sharing content (or engaging in conduct) that is radicalised, extremist, racist, anti-Semitic or discriminatory in any other way.
- Using digital tools or technologies (including artificial intelligence) in a way that is deceptive, abusive or intended to cause harm to others.

This is not an exhaustive list. The school reserves the right to amend this list at any time. The headteacher (or delegated senior leader) will determine whether behaviour not listed above constitutes unacceptable use.

Unacceptable use may result in restricted access to ICT systems, suspension of network access, and/or further action in line with the school's disciplinary procedures.

4.1 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. With express written permission from the headteacher.

4.2 Sanctions

Students and staff who engage in any of the unacceptable activity listed above may face disciplinary action in line with

Where acceptable use policy is not followed network and/or internet access can be suspended or removed, in addition to any other sanctions applied in line with school policies

5. Staff (including governors, volunteers, and contractors)

5.1 Access to school ICT facilities and materials

The school's ICT team, led by the network manager, manage access to the school's ICT facilities for 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 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 ICT teamvia Helpdesk@oldfieldschool.com

5.1.1 Use of phones and email

The school provides each member of staff with an email address, for which multi-factor authentication is used.

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 and students, 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.

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 network manager immediately and follow our data breach procedure.

Staff must not give their personal phone numbers to parents or students.

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.

5.2 Personal use

Staff are permitted to 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 ICT team will give 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.
- Does not constitute 'unacceptable use', as defined in section 4.
- Takes place when no students are present.
- Does not interfere with their jobs, or prevent other staff or students from using the facilities for work or educational purposes.

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 must maintain clear professional boundaries when using digital communication and must not use school ICT systems in ways that blur professional and personal roles.

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 students 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 (see section 5.1.1) to protect themselves online and avoid compromising their professional integrity.

5.2.1 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 social media accounts (see appendix 1).

5.3 Use of school laptops and cloud-based systems

All staff are issued with a school-owned laptop for professional use.

Staff access school documents and resources through approved cloud-based systems, including the school's SharePoint environment, using their school-issued accounts. No remote desktop or remote access software is used to connect to the school network.

When using school laptops on or off site, staff must:

- Use only school-approved accounts and systems to access school data
- Ensure devices are kept secure, password-protected and locked when not in use
- Take reasonable steps to prevent unauthorised access to devices or information, particularly when working off site or in shared environments
- Store school data only within approved systems and not on personal devices or unapproved cloud services
- Report the loss, theft or suspected compromise of a school device or account immediately to the Network Manager

All use of school laptops and cloud-based systems is subject to the same monitoring, data protection and acceptable use requirements set out in this policy and the school's Online Safety Policy.

5.4 School social media accounts

The school has official social media accounts, managed by the school's Events Manager. Staff members who have not been authorised to manage, or post to, the account, must not access, or attempt to access the accounts.

The school has guidelines for what can and cannot be posted on its social media accounts. Those who are authorised to manage the account must ensure they abide by these guidelines at all times.

5.5 Monitoring of school network and use of ICT facilities

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
- 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

6. Students

6.1 Access to ICT facilities

- Computers and equipment in the school's ICT suite are available to students in years 7 to 11 only under the supervision of staff
- The use of laptops in department-based laptop banks by students is managed by the teachers in that department.
- Sixth-form students can use the schooldesktop computers independently for educational purposes.
- Sixth form students are able to register one personal device that is connected to the school WiFi network.
- Students in Years 7 to 11 may be allowed to register a personal device that is connected to the school WiFi network if they have individual requirements, as agreed by Network manager.
- Specialist ICT equipment, such as that used for music, or design and technology, must only be used under the supervision of staff
- Students will be provided with an Office365 account which provides them with an email address and access to Office365 apps (including the school SharePoint site).
- Students may be issued with school-owned laptops for use in lessons and/or at home as appropriate.

6.2 Search and deletion

Under the Education Act 2011, and in line with the Department for Education's guidance on searching, screening and confiscation, the school has the right to search students' phones, computers or other devices for pornographic images or any other data or items banned under school rules or legislation.

The school can, and will, delete files and data found on searched devices if we believe the data or file has been, or could be, used to disrupt teaching or break the school's rules.

Staff members may also confiscate devices for evidence to hand to the police, if a pupil discloses that they are being abused and that this abuse contains an online element.

6.3 Unacceptable use of ICT and the internet outside of school

The school will sanction students, in line with the behaviour/discipline policy, 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 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 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, other students, 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 ICT facilities or materials
- 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

7. Parents

7.1 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 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 are granted access in this way, they must abide by this policy as it applies to staff.

7.2 Communicating with or about the school online

We believe it is important to model for students, 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.

8. 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, students, parents and others who use the school's ICT facilities should use safe computing practices at all times.

8.1 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.

Members of staff or students 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.

8.2 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.

8.3 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 SIMS Connected should only be made on a school owned device, if any member of staff wishes to use a personally owned device then this will need to be requested in advance from the Network Manager.

8.4 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 school ICT 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 Network Manager 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.

8.5 Encryption

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

School staff may only use personal devices 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, as defined by the Network Manager.

9. Protection from cyber attacks

The school will:

- Work with governors and the IT department to make sure cyber security is given the time and resources it needs to make the school secure
- Provide training for staff (and include this training in any induction for new starters, if they join outside of the school's 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:
    - **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 up to scratch and secure as they can be
- Back up critical data daily (overnight and store these backups on on-site servers in Server room and the Drama Block.
- Back up critical data monthly (at end of each month and store these backups on external hard drive kept by the Network Manager off-site. This hard drive is encrypted and data can only be accessed through the backup server software and requires a password.
- Delegate specific responsibility for maintaining the security of our management information system (MIS) to ESS (Education Software Solutions).
- 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 (Disaster Recovery 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 Action Fraud of the incident. This will be reviewed and tested every 12 months and after a significant event has occurred, using the NCSC's 'Exercise in a Box'.

10. Internet access

The school wireless internet connection is secured.

- The school's site wide WiFi connection for school owned and BYOD (bring your own device) is subject to the same web filtering and monitoring as wired connected computers
- BYOD access is granted to sixth form students and staff only. However, it may be granted in exceptional circumstances to other stdueunst who have a specific need.

If a member of staff notices that an inappropriate web site has not been filtered they should report the web address to the Network Manager via helpdesk@oldfieldschool.com .

The safeguarding software (classroom.cloud) flags inappropriate usage of school devices. These reports are reviewed by the ICT Team and where necessary addresses are blocked.

10.1 Students

- The schools wifi for BYOD is available for sixth form students and covers the whole school site. Students will be required to register their devices using their school network accounts in order to connect
- Any security or filtering settings you use All internet usage including BYOD devices are subject to internet filtering and monitoring
- How students can request access Students will be provided instructions by email on how to access the schools BYOD wifi service
- What the use of wifi is limited to Students are unable to access social media site via the school wifi.

10.2 Parents and visitors

Parents 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 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.

11. Monitoring and review

The deputy headteacher and Network Manager monitor the implementation of this policy, including ensuring it is updated to reflect the needs and circumstances of the school.

The governing board is responsible for approving this policy.

12. Related policies

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

- Online safety
- Safeguarding and child protection
- Behaviour
- Staff discipline
- Staff code of conduct
- Data protection
- Remote learning
- Mobile phone usage
- BYOD
- Data Breach policy

Appendix 1: Acceptable use policy for students

Students must agree to this each time they log in to a school computer.

Oldfield School – ICT Acceptable Use Policy

As a student at Oldfield School you are entitled to use the ICT facilities, but you must do so in a safe and responsible way. The school monitors computer use and may check files, emails and internet activity at any time.

Usernames and Passwords

- Never use a username or password allocated to another person.
- Never share your password – you are responsible for all activity on your account.
- Choose a password that is easy for you to remember but hard for others to guess.
- If you forget your password, ask your ICT teacher or an ICT Technician for help.

Responsible Use

- ICT facilities are for schoolwork and learning – other use is not normally allowed.
- Always be polite and respectful online – no cyberbullying or offensive messages.
- Do not share personal details (address, phone number etc.) with people you do not know.
- Do not try to access blocked websites, bypass security, or install software.
- Game playing is only allowed when a teacher says so in a lesson.

Good Working Practice

- Log off when you finish using a computer.
- No food or drink near computers – keep the area tidy.
- Report technical problems to ICT staff or your teacher – do not attempt fixes yourself.
- Leave rooms tidy and give up a computer if another class arrives.

Printing

- Check what you are printing – only print what you need.
- Your print jobs stay in the queue for 72 hours and then are deleted.
- You have a set number of printer credits each term – use them sensibly.

If Things Go Wrong

If these rules aren't followed, your ICT access may be restricted for a time and you may be asked to discuss the issue with your teacher or a member of staff so it can be put right.