ICT and Internet Acceptable Use Policy

Date of last review:	2024	Review period:	3 Years
Date of next review:	2027	Written by:	Rebecca Garratt
Type of policy:	Non-statutory	Committee:	FGB
Signature:			

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 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 and visitors.

Breaches of this policy may be dealt with under staff code of conduct

2. 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 2023

- 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

3. 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.

4. 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

- 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 Technical Support

- 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 to write homework or class assignments

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

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.

- Pupils may use AI tools and generative chatbots where those tools have been provided by the school:
  - 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.

4.2 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 or staff code of conduct

Flagrant disregard for the rules in this document may be considered gross misconduct and in extreme cases may result in reports being made to relevant authorities such as the ICO, Police, etc.

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

5.1 Access to school ICT facilities and materials

The school's network manager 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 are expected to keep this login secure and not write it down anywhere in its entirety. Staff must lock or log off devices when they are not in use. Staff must not share passwords or use other staff members user accounts under any circumstances.

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 network manager.

Requests to elevate privileges or provide additional access will be reviewed by the network manager and for more sensitive access, passed through the headteacher for approval.

5.1.1 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.

Staff must take extra care when sending sensitive or confidential information by email.

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 School Business Manager 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 and vice versa

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

Whilst devices provided for you are intended for the sole purpose of conducting your work whilst at WFS, Staff are permitted to occasionally use school ICT facilities for personal use, for example online shopping. This is subject to certain conditions set out below. This permission must not be overused or abused. The network manager may withdraw or restrict this permission at any time and at their discretion.
Due to the sensitive nature of materials available to you this benefit strictly does not extend to anybody else, including immediate family members.

Personal use is permitted provided that such use:

Does not take place during class 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.

Personal devices should be kept secure and out of sight. They should not be used in live classrooms but may be used in PPA or Staff workrooms when on breaks. For emergency contact purposes (for example from your children's childcare provider) you may use the main school number and your extension number, alternatively reception staff will always pass along any urgent messages. On rare occasions permission can be sought from the Headteacher to have their personal phone o their person but not in view of pupils.

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 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 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 Social media accounts (see appendix 1).

5.3 Remote access

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 school 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.

5.4 School social media accounts

The school has official social media accounts. Staff members who have not been authorised to manage, or post to, the accounts must not access, or attempt to access, the account. If staff wish to use or create social media pages/channels the permission should be sought from the headteacher.

5.5 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

- Search terms entered

- 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

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

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.

6. Pupils

6.1 Access to ICT facilities

Computers and equipment in the school are available to pupils only under the supervision of staff. We also have specialist ICT equipment, such as that used in sensory areas or SEND specific devices.

Sixth-form pupils are issued with laptops they may use independently, for educational purposes only.

Boarding students have access to devices that they can use in their leisure time.

6.2 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 **and/or**

- 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 headteacher / designated safeguarding lead

- Explain to the pupil why they are being asked to be 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 – the search will only be carried out by a member of SLT with another member of staff and only if pupil agrees. If the pupil disagrees the parent must be contacted and come into school immediately.

- 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.

- Involve the DSL (or deputy) without delay if they believe that a search has revealed a safeguarding risk

SLT 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 the senior leadership team 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:

- 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 policy / 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.

6.3 Unacceptable use of ICT and the internet outside of school

The school will sanction pupils, in line with the behaviour 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 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

7. Parents/carers

7.1 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 Friends of WFS) 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.

7.2 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.

7.3 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.

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.

8. 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 and web filtering 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 are responsible for the security of their passwords and accounts, and for setting permissions for accounts and files they control. Users should not write complete usernames and passwords down anywhere. Partial details/hints are acceptable.

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.

The Technical Support department are responsible for issuing usernames and passwords to both staff and students and should be approached if any details are incorrect or need changing.

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 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.

WFS Technical support staff do not support connection of any personal devices to the schools' network.

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.

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 Technical Support in conjunction with the headteacher where elevated privileges are required.

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 Technical Support immediately.

Users should always log out of systems and lock their equipment when they are not in use to avoid any unauthorised access

8.5 Encryption

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

Personal devices (including computers and USB drives) should not be used to access school data, work remotely, or take personal data (such as pupil information) out of school.

9. 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 department 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 objectively test that what it has in place is effective

    - **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 daily and store these backups on-premises and ensure they are robust and regularly tested to guarantee retrieval if needed.

- 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 and providing appropriate filtering

- Develop, review and test an incident response plan with the IT department including, for example, how the school will communicate with everyone if communications go down, who will be contacted and when, and who will notify Action Fraud of the incident. This plan will be reviewed and tested and after a significant event has occurred, using the NCSC's 'Exercise in a Box'

- Work with our LA to see what it can offer the school regarding cyber security, such as advice on which service providers to use or assistance with procurement

10. Internet access

The school's wireless internet connection is secured with state of the art filtering and monitoring.

Guests can request a login slip which provides short term access to the internet

All access to the internet is monitored for cybersecurity and safeguarding reasons.

11. Acceptable User Policy

At WFS all staff, parents/carers, governors and volunteers are expected to sign and adhere to the AUP Agreement (appendix 4) and visitors will abide by the notice on the access slip.

Due to the cognitive levels of the pupils at WFS there are different expectations dependent upon need. 6th Form (where appropriate) will sign and adhere to their AUP and Pathway 3 & 4 to theirs. Early Years, Pathway 1 and Pathway 2 have limited access to ICT and are not expected to sign an AUP Agreement.

12. Monitoring and review

The headteacher and Technical Support department 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 2 years.

The governing board is responsible for reviewing/approving this policy.

13. Related policies

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

- Online safety
- Safeguarding(including child protection)
- Behaviour
- Disciplinary
- Data protection
- Remote learning policy
- Mobile phone