GIRLINGTON PRIMARY SCHOOL

ICT and internet acceptable use policy

Date Policy Written:	Spring 2024
Date Policy Ratified:	Spring 2024
Date Policy to be Reviewed:	Spring 2026

Introduction and aims

ICT is an integral part of the way our school works, and is a critical resource for pupils, staff, 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 can 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 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 code of conduct/ disciplinary 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](#)
- [Searching, screening and confiscation: advice for schools](#)

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, 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

- Accessing, creating, storing, linking to or sending material that is pornographic, offensive, obscene or otherwise inappropriate

- 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

This is not an exhaustive list. The school reserves the right to amend this list at any time. The head teacher or the online safety team 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.

Exceptions from unacceptable use

Where the use of school ICT facilities is required for a purpose that would otherwise be considered to be classed as unacceptable use, exemptions to the policy may be granted at the head teacher's discretion and a proposal made to the online safety team.

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 on code of conduct/ disciplinary policy.

Staff (including governors, volunteers, and contractors)

Access to school ICT facilities and materials

The school's ICT Technician 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 log-in/account information and passwords that they must use when accessing the school's ICT facilities.

Staff who have access to files/drives they are not authorised to view or edit, or who need their access permissions updated or changed, should contact their line manager or the head teacher

Use of phones and email (also see separate Mobile Phone and Camera Policy and Online Safety Policy)

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 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. Any attachments containing sensitive or confidential information should be encrypted so that the information is only accessible by the intended recipient. Staff should be using Galaxkey email system if sending documents outside of school.

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 which contains the personal information of another person, they must inform the Deputy Head Teacher / ICT Technician immediately and follow our data breach procedure.

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 unless authorised by the Head teacher.

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.

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 Head teacher 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 directed 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 are also permitted to use their personal devices (such as mobile phones or tablets) in line with the school's mobile phone and camera policy.

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

Personal social media accounts

Members of staff should ensure that 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.

Any request for remote access is made to the line manager and the Head teacher.

Once the request has been granted the ICT technician will set up remote access for the staff member on the server. The technician will provide instructions on how the staff member will be able to access the school network from home.

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 take such precautions as the ICT Technician may require from time to time 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. Please see Data Protection Policy.

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
- 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

Pupils

Access to ICT facilities

Computers, laptops and ICT equipment in the school are available to pupils only under guidance and permission of staff. Specialist ICT equipment, such as that used for music, science 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, in line with the behaviour and 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
- 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 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

Sanctions will apply according to the school's behaviour and positive discipline policy.

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 PTA - Parent Teacher Association) may be granted an appropriate level of access, or be permitted to use the school's facilities at the Head teacher's discretion.

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

Data security

The school 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.

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.

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.

School's data protection – GDPR policy available in the Staff Handbook drive.

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 ICT technician.

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 ICT technician 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 (See Online Safety Policy)

All school devices that hold data (as defined by the Data Protection Act 1998) are encrypted using Bitlocker. No unencrypted device i.e laptop, or USB drive is to leave the school premises.

Staff to only use school laptops /USB to access the school network either at school or when working remotely from home.

The school ensures 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 head teacher.

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

Internet access

We use Netsweeper web filtering and reporting software which is provided by Schools Broadband who are part of the Internet Watch Foundation (IWF).

The school has separate web filtering for Staff and pupils. The Netsweeper filtering software prevents unauthorized access to illegal websites, it also prevents access to inappropriate websites. The school has control to filter themselves to permit or deny access to specific websites. The filtering system is applied on the network and has the ability to provide information on websites visited by users.

Securus is a computer monitoring and reporting software used by the school. If a child is in breach of their acceptable use agreement whilst on the computer then an email is sent to the designated people with a screen shot of the incident showing what was displayed at that time and who was involved.

WIFI

The school currently has two WIFI SSID's which are both part of the school web filtering system. One WiFi SSID is used by all school staff, and the other is used by guests to the school (i.e training course in school), The guest Wifi is for internet use only and not part of the school network

Both the WiFi SSID's are WPA2 encrypted and require a password.

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 head teacher.

The head teacher 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 guest wifi only, 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.

Monitoring and review

The head teacher and the online safety team monitor the implementation of this policy, including ensuring that it is updated to reflect the needs and circumstances of the school.

This policy will be reviewed every two years.

The governing board is responsible for approving this policy.

Related policies

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

- Online safety
- Safeguarding and child protection
- School Behaviour - Positive Discipline Policy
- Staff discipline
- Data protection/GDPR
- Mobile Phone and Camera Policy
- Code of Conduct
- CCTV Schools Security Policy

Don't accept friend requests from pupils on social media

10 tips 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 wifi connections and makes friend suggestions based on who else uses the same wifi connection (such as parents or pupils)

Check your privacy settings

- Change the visibility of your posts and photos to **'Friends only'**, rather than 'Friends of friends'. Otherwise, pupils and their families may still be able to read your posts, see things you've shared and look at your pictures if they're friends with anybody on your contacts list

- Don't forget to check your **old posts and photos** – go to bit.ly/2MdQXMN to find out how to limit the visibility of previous posts

- The public may still be able to see posts you've **'liked'**, even if your profile settings are private, because this depends on the privacy settings of the original poster

- **Google your name** to see what information about you is visible to the public

- 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 do to 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 head teacher about what's happening

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

Girlington Primary Student

Pupil Acceptable Use Policy Agreement – for older pupils

This is how we stay safe when we use computers:

- I understand that I am responsible for my own actions.
- I will use my knowledge of internet safety to guide me whenever and wherever I am online.
- I will only use the network, Internet and e-mail when a teacher has given permission.
- I will only access the network with the login and password I have been given and I will keep my password secret.
- I will not access other people's files without their permission.
- I understand that the school will check my computer files and monitor the internet sites I visit.
- I will not copy anyone's work and call it my own.
- I will not bring in software from outside school and try to use it on the school computers.
- I will only e-mail people I know, or a teacher has approved.
- I will be polite and responsible when sending e-mail and will not forward any chain letters.
- I will not give any personal details to anyone on the Internet or in any e-mail or arrange to meet anyone out of school.
- I will report any unpleasant material to a teacher immediately because this will help protect other pupils and myself.
- I will discuss internet safety issues with my parents or carers and uphold any rules for safe internet use in my home.
- I know that if I break the rules I might not be allowed to use a computer.

Girlington Primary Student

Pupil Acceptable Use Policy Agreement – for younger pupils

This is how we stay safe when we use computers:

- I will ask a teacher or suitable adult if I want to use the computers
- I will only use activities that a teacher or suitable adult has told or allowed me to use.
- I will take care of the computer and other equipment
- I will ask for help from a teacher or suitable adult if I am not sure what to do or if I think I have done something wrong.
- I will tell a teacher or suitable adult if I see something that upsets me on the screen.
- I will keep my passwords and login details a secret so no one else will know them.
- I know that if I break the rules I might not be allowed to use a computer.

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   - Leave my desktop unlocked if I leave the classroom and only use a computer that I am logged into with my own username and password.   - 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.   - 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.

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