new wave federation

Staff Acceptable Use of Technology Policy 2025 - 2026

Kindness

Focus

Creativity

Responsibility

Collaboration

Introduction and Aims

ICTis an integralpartof the way our school worksand 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 also pose safeguarding, data protection and online safety risks.

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 engagement with varied sources of digital technology.

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 staff code of conduct.

Staff Access to school ICT facilities and materials

Access to school ICT facilities and materials

The school's IT management service, Turn IT On manage access to the school's ICT facilities and materials for school staff including our hardware such as computers and Chromebooks. In addition to this they manage our logins and accounts across all hardware and software.

Our school iPads are managed by another service provider, Sync. Our internet - wired connections and WIFI- is provided by London Grid for Learning (LGfL).

Sync and Turn IT On both review and report directly to senior leaders and the designated safeguarding lead regarding access to hardware and software as well as the use of internet when connected to the school's broadband.

Staff will be provided with unique login/account information and passwords that they must use when accessing the school's ICT facilities. These should never be shared with colleagues or external visitors 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 Turn IT On.

Staff are permitted to use their personal devices (such as mobile phones or tablets) in the staffroom, offices, and in other areas once the children are off site. They are not permitted to use these in corridors or during lesson time and these devices must be locked away and must not be kept in pockets during the school day.

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.

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. These should be marked using the terminology "SENSITIVE/HIGHLY SENSITIVE". Any attachments containing sensitive or confidential information should be encrypted so that the information is only accessible by the intended recipient. Senior Leaders can provide additional support on sending encrypted emails with secure data software such as Egress.

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 headteacher and Turn It On technician immediately who will proceed to follow our data breach procedure.

Staff must not give their personal phone number(s) to parents/carers or pupils and staff must never call families using their personal device to telephone families, even if the number is withheld.

Staff must not check their emails on any device whilst children are present in the vicinity, including in classrooms, offices and whilst on school outings.

Personal social media accounts

Staff should maintain appropriate social media use for both professional and personal purposes. Personal ICT use, even outside of school facilities, can affect employment if it reveals personal details publicly. To safeguard their privacy, staff must review and secure their digital accounts, particularly social media, ensuring that pupils and families cannot access theirpersonal information.

Use of artificial intelligence (AI)

Staff should be aware of the risks of usingAI tools whilst they are still being developed. Teaching staff are not permitted to use AI for teaching and learning purposes without expressed permission from the headteacher. Should a decision be made to use it, then staff members should carry out a risk assessment where new AI tools are being used.

Remote access (Offsite)

Staff can access the school's ICT resources remotely using assigned devices like iPads or laptops with their Google accounts. They must follow the same rules as if they were on-site. Extra caution is required for remote access, including securely storing devices, keeping them password-protected, and not leaving them unattended in public. ICT environments, like Google Drive shared drives, contain confidential information protected by data protection laws and must be handled according to our data protection policy.

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

To ensure child safety and welfare, the school may filter and monitor its ICT facilities and network. This includes, but is not limited to, overseeing:

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

Authorised ICT personnel, the headteacher and the Designated Safeguarding Lead and their deputies may filter, inspect, monitor, intercept, assess, record and disclose the above, to the extent permitted by law.
The school monitors ICT use in order to:

- Safeguard children and young people;
- 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 are 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 concern;
- 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.

Acceptable use of the school's ICT systems and internet: agreement for staff, governors, volunteers and visitors
Name of staff member/governor/volunteer/visitor:_____
When using the school's ICT systems and accessing the internet in school, or outside school on a work device (such as a teacher iPad), 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 using personal accounts; • Post material, images or information that could identify children and their school on any websites, including social media; • 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; • Take photographs, record video or gather any information that could otherwise identify individual children on a personal device; • Take photographs, record video or gather any information that could otherwise identify individual children on a sanctioned school device, without ascertaining parental permissions; • 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 will only use the school's ICT systems and access the internet in school, or outside school on a work device, for educational purposes or for the purpose of fulfilling the duties of my role. I agree 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 both outside and inside of 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 (Turn IT On) 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 :	**Date:**