



Glenfield Primary School

Acceptable Use Agreement

Date of Review	September 2026
Next Review Date	September 2027
Headteacher	Sukhi Tibbles
Chair of Governors	Tessa Wildgoose

1. Introduction

1.1 This Acceptable Use Policy is intended to provide a framework for such use of the School's ICT Infrastructure. It should be interpreted to have the widest application, including new and developing technologies and uses, which may not be explicitly referred to.

1.2 This policy has due regard to all relevant legislation and statutory guidance including, but not limited to, the following:

- Computer Misuse Act 1990;
- UK General Data Protection Regulation (UK GDPR) and Data Protection Act 2018;
- Counter-Terrorism and Security Act 2015;
- Prevent duty guidance: England and Wales (2023);
- Keeping Children Safe in Education 2026
- Working Together to Safeguard Children 2026;
- Guidance for safer working practice for those working with children and young people in education settings

1.3 As a professional organisation with responsibility for safeguarding, all staff within Glenfield Primary School are expected to take all possible and necessary measures to protect data, information systems, and devices from damage, loss, unauthorised access, infection, abuse, and theft.

1.4 All users of the School's ICT Infrastructure have a responsibility to use the school's computer systems in a professional, lawful, and ethical manner, consistent with the school's ethos, national/local guidance and expectations, the law, and relevant School and academy policies including:

- Employee Code of Conduct;
- Data Protection Policy;
- Online Policy;
- Disciplinary Policy;
- Safeguarding Policy.

2. Responsibilities

It is the responsibility of all users of Glenfield Primary School to read and understand this policy. This policy is reviewed on an annual basis but is liable for amendments more frequently to comply with changes in governance to address technology trends.

3. Scope

Members of the School and all other users (staff, students, trustees, governors, volunteers, visitors, contractors, and others) of the School's facilities are bound by the provision of its policies in addition to this ICT Acceptable Usage Policy.

4. System Security and Policy

4.1 Hardware and software provided by the workplace for staff and students' use can only be used for educational use. Personal accounts or information such as personal photographs or personal files should not be accessed or stored on school devices, and the School accepts no liability for the loss of such data.

4.2 Downloading or accessing programs or files that have not been authorised by the Head of Shared Services or IT Business Partner could result in the activation of malware or ransomware when devices are reconnected to school networks. If in doubt, users should ask the IT team for guidance. Where there is a resultant breach, users may be individually liable for such a breach.

4.3 Users must not remove or attempt to inhibit any software placed on school devices that are required by the School for network compliance or security.

4.4 Users must not attempt to bypass any filtering and/or security systems put in place by the School.

4.5 Damage or loss of a computer, system, or data including physical damage, viruses, or other malware must be reported to the IT team as soon as possible.

4.6 The School reserves the right to monitor the activity of users on any of its ICT systems and devices and all devices should be considered monitored.

4.7 Password security is important. Get Safe Online provides guidance on password security and recommends Do's and Don'ts.

4.8 Equipment remains the property of Glenfield Primary School. The School may request the return of any equipment for any reason at any time by giving appropriate notice. If staff are leaving employment of the School, staff must return equipment prior to the leaving date. Students leaving education who have been issued devices must return devices on their last day.

4.9 The School ICT infrastructure may not be used directly or indirectly by any user for any activity which is deemed to be unacceptable use, consisting of, but not limited to, the following definitions:

- The download, creation, manipulation, transmission, or storage of any offensive, obscene, or indecent images, data, or other material, or any data capable of being resolved into obscene or indecent images or material;
- Unlawful material, or material that is defamatory, threatening, discriminatory, extremist, or which has the potential to radicalise themselves or others;
- Unsolicited "nuisance" emails, instant messages, or any other form of communication;
- Material which is subsequently used to facilitate harassment, bullying, and/or victimisation of a member of the School or a third party;
- Material which promotes discrimination on the basis of race, gender, religion or belief, disability, age, or sexual orientation;
- Material with the intent to defraud or which is likely to deceive a third party;
- Material which advocates or promotes any unlawful act;
- Material that infringes the intellectual property rights or privacy rights of a third party, or that is in breach of a legal duty owed to another party;
- Material that brings the School into disrepute;
- Using the School ICT Infrastructure deliberately for activities having, or likely to have, any of the following characteristics:
 - Intentionally wasting staff effort or other School resources;
 - Corrupting, altering, or destroying another User's data without their consent;
 - Disrupting the work of other Users or the correct functioning of the School ICT Infrastructure;
 - Denying access to the School ICT Infrastructure and its services to other users;
 - Pursuance of personal commercial activities.

5. Data Protection

5.1 Staff must be aware of their responsibilities under Data Protection legislation (including UK GDPR and the Data Protection Act 2018) regarding personal data of pupils, staff, or parents/carers. This means that all personal data must be obtained and processed fairly and lawfully, kept only for specific purposes, held no longer than necessary, and kept private and secure with appropriate security measures in place, whether used in the workplace, hosted online, or accessed remotely. This includes safe and secure backup.

5.2 Staff should seek to use designated school systems to store, manage, process, or view personal information wherever possible to ensure security of information, appropriate deletion and archiving, and to ensure that searches in response to Subject Access Requests can easily and readily be completed. Data

must not be extracted from these systems and installed in personal spreadsheets or documents unless absolutely necessary.

5.3 Emails, text messages, Teams posts created or received as part of your role are subject to disclosure in response to a request for information under the Freedom of Information Act 2000 or a Subject Access Request under the Data Protection Act 2018. All e-mails, texts, and messages should be written and checked carefully before sending, in the same way as a letter written on school-headed paper. Do not use data subjects' (staff, students, parents, contractors) names in communications unless absolutely required. Where appropriate, use initials. All electronic communications with students, parents, outside agencies, and staff must be compatible with the professional role of staff. The person about whom a communication relates may request copies of the information therein.

5.4 Staff are reminded that any sharing of data with third parties should be subject to scrutiny by the School's Data Protection Lead to ensure an appropriate GDPR-compliant data sharing agreement and appropriate licensing are in force. If you are not aware of whom your location's data protection lead is, please contact the senior administrator, school operations manager, or the Head of Shared Services who will be able to inform you who the relevant person is.

5.5 Staff must not keep school-related personal information, including sensitive information, images, files, videos, or emails, on any non-School issued devices unless approval has been granted by the Head of Shared Services or IT Business Partner prior to the start of any activity.

5.6 Users should use appropriate School platforms (such as Office 365 or Teams) to access work documents and files in a password-protected environment.

5.7 Staff are not permitted to use USB sticks to connect to any School device; no data is permitted to be stored on USB sticks unless explicit approval has been granted by the ICT lead.

5.8 Any images or videos of students must only be for official School use and reflect parental or age-appropriate student consent. Staff should ensure photos and videos are regularly uploaded to a shared network or official cloud drive, regularly deleted in line with retention policies, and removed from standalone devices.

5.9 Users are expected to respect copyright and intellectual property rights.

5.10 Staff must use School-provided accounts for all official communication; personal accounts must never be used. It is the responsibility of each account holder to keep the password secure. For the safety and security of users and recipients, all mail is filtered and logged. If necessary, e-mail histories can be traced. The school email account should be the account that is used for all school business. Under no circumstances should staff contact students, parents, or conduct any school business using personal e-mail addresses.

5.11 Staff should actively manage e-mail accounts, delete e-mails of short-term value, and carry out frequent housekeeping on all folders and archives.

6. Safeguarding

6.1 Staff are expected to immediately report any illegal, inappropriate, or harmful material or any incidents they become aware of to a Designated Safeguarding Lead.

6.2 Queries or questions regarding safe and professional practice online either in an academy or off-site should be raised with a Designated Safeguarding Lead, your local Headteacher, or HR.

7. Consequences

Glenfield Primary School may:

7.1 Restrict or terminate a User's right to use the School's ICT Infrastructure;

7.2 Withdraw or remove any material uploaded by that User in contravention of this Policy;

Disclose information to law enforcement agencies and take any legal action against a User for breach of this Policy, including but not limited to claiming all costs, fees, and disbursements (including but not limited to legal fees) connected therewith; or

Where the User is also a member of the School community, the School may take disciplinary action up to and including expulsion from study or termination of employment.

8. Monitoring

All School ICT systems and devices are monitored in accordance with policy, so personal privacy cannot be assumed when using School hardware or systems. The School can monitor the usage of its own Infrastructure and services (internet access, email, Teams, WiFi, etc.) as well as activity on end-user compute (Tablets, Laptops, Desktop computers, mobile phones, etc.) without prior notification or authorisation from Users when justifiable concerns have been raised. This will be in line with the School's Investigation procedure.

8A. Filtering and Monitoring

8A.1 The School will have appropriate filtering and monitoring systems in place to safeguard pupils and staff from potentially harmful and inappropriate online material. Filtering and monitoring arrangements will reflect the age range and needs of pupils, the devices and services in use, and the specific safeguarding risks within each setting.

8A.2 Roles and responsibilities for filtering and monitoring will be clearly identified. The effectiveness of filtering and monitoring provision will be reviewed at least annually, and more frequently where there is a significant change to technology, provision or identified risk.

8A.3 Users must not attempt to bypass, disable or interfere with filtering, monitoring, security or safeguarding controls. Any concerns about over-blocking, under-blocking, inappropriate content, alerts or the effectiveness of monitoring must be reported promptly through the School's agreed reporting route.

8A.4 Staff must understand that filtering and monitoring systems do not replace professional vigilance. Any safeguarding concern identified through online activity, including content viewed, searched for, created, shared or communicated, must be reported in accordance with the School's safeguarding procedures.

8B. Generative Artificial Intelligence (AI)

8B.1 Generative artificial intelligence (AI) tools, including tools that generate text, images, audio, video or other content, must only be used for School business where their use is appropriate, lawful, safe and consistent with School policies and any approved local arrangements.

8B.2 Staff must not enter personal data, special category data, confidential information, safeguarding information, assessment information that identifies an individual, passwords, security information or other sensitive School information into a generative AI system unless the School has specifically approved the system and the proposed use, including its data protection arrangements.

8B.3 Users remain professionally responsible for any content produced with the assistance of AI. AI-generated content must be checked for accuracy, appropriateness, bias, safeguarding concerns, copyright or intellectual property issues and suitability before it is relied upon, shared or used in School work.

8B.4 AI must not be used to make autonomous decisions about pupils, staff or other individuals where those decisions could have a significant effect on them. Appropriate human oversight and professional judgement must always be maintained.

8B.5 Any use of AI with or by pupils must be age-appropriate, appropriately supervised and consistent with the School's safeguarding, online safety, filtering and monitoring arrangements. Staff should follow current Department for Education guidance on the safe and effective use of generative AI in education.

8C. Personal Devices, Messaging and Online Communication

8C.1 Personal devices must not be used to photograph, film or record pupils, or to store pupil or School information, unless expressly authorised for a specific purpose under an agreed School procedure.

8C.2 Staff must use School-approved communication systems and accounts when communicating with pupils, parents/carers, colleagues and external agencies about School business. Personal social media accounts, personal messaging accounts and personal email accounts must not be used for professional communication unless an expressly approved School arrangement applies.

8C.3 Staff must maintain appropriate professional boundaries in all online communication and must not engage in online contact with pupils that could compromise safeguarding, confidentiality or professional standards.

8D. Cyber Security and Incident Reporting

8D.1 Users must take reasonable steps to protect School systems and information from cyber security risks, including phishing, malicious links or attachments, unauthorised software, compromised passwords and attempts to gain unauthorised access.

8D.2 Suspected phishing, malware, ransomware, loss or theft of a device, accidental disclosure of information, compromised accounts, unusual system activity or any other suspected cyber or data security incident must be reported immediately through the School's agreed IT and/or data breach reporting procedures.

8D.3 Users must follow School requirements for passwords, authentication and account security and must never share passwords or authentication codes with another person.

8E. Online Safety and Emerging Technology

8E.1 Online safety is a safeguarding responsibility. Users must remain alert to the four broad areas of online risk: content, contact, conduct and commerce, and must report concerns in accordance with the School's safeguarding procedures.

8E.2 This agreement applies to new and emerging technologies, platforms and forms of online communication whether or not they are specifically named in this document. Where there is uncertainty about whether a technology or service is appropriate for School use, users must seek advice before using it for School business or with pupils.

9. Agreement

9.1 Staff will be made aware of significant changes to this agreement and associated safeguarding, online safety, filtering and monitoring expectations. The School may require staff to confirm that they have read and understood updated requirements following review.