Acceptable Use of ICT Policy

Implementation Date: November 2026

Review Date: November 2027

Purpose

ICT in its many forms, including internet access, email, cloud-based systems, artificial intelligence tools and mobile devices, are an integral part of school life. Wheelock Primary School is committed to ensuring that all ICT is used safely, responsibly and professionally.

Acceptable Use Responsibilities

All staff, governors and visitors understand that:

- ICT includes a wide range of systems, including computers, laptops, tablets, mobile phones, cloud-based services and digital communication platforms.
- School ICT equipment must only be used for authorised educational and professional purposes.
- Passwords must never be shared with others.
- Users are responsible for all activity undertaken through their accounts.
- Hardware or software must not be installed on school devices without authorisation.
- Internet activity on school-owned systems may be monitored and recorded.
- Online safety concerns must be reported to the Designated Safeguarding Lead or Deputy DSL immediately.
- School email systems and approved communication platforms must be used for all school business.
- Personal email accounts must not be used for school purposes.
- School data must be protected and handled in accordance with UK GDPR and the Data Protection Act 2018.
- School information should only be stored on approved school systems and cloud storage platforms.
- Encryption must be used where appropriate.
- Artificial Intelligence (AI) tools must only be used responsibly and in line with school guidance. Personal or confidential information must not be entered into public AI systems.
- Staff must not browse, download, upload or distribute material that could be considered offensive, discriminatory or illegal.

- Copyright and intellectual property laws must be respected.
- Staff must not discuss pupils, families, colleagues or confidential school matters on personal social media accounts.
- Use of the school's Facebook account must comply with the school's Social Media Policy.

Personal Devices and Mobile Phones

- Personal devices may only be used for school business with the permission of the Headteacher.
- Personal mobile phones must never be used to photograph or record pupils.
- School iPads and devices must only be used for school purposes.
- Pupils who bring mobile phones to school must ensure that they are switched off and handed into the school office before registration.
- Mobile phones will be stored securely by the school office during the school day and returned at the end of the school day.

Security Requirements

Staff members must ensure that:

- School devices are not left unattended.
- Devices automatically lock after a period of inactivity.
- Strong passwords are used.
- Passwords are changed when required.
- Multi-Factor Authentication (MFA) is used where available.
- School devices are only taken off-site for authorised purposes, including home working, school visits and professional development activities.
- School information is accessed securely when working remotely.

Reporting Concerns

Any concerns relating to:

- inappropriate use of technology,
- cyber security incidents,
- data breaches,
- online safety concerns,
- safeguarding concerns,

must be reported immediately to the Headteacher or a member of the Safeguarding Team in accordance with school policies.

Monitoring and Review

This policy will be reviewed annually or sooner if required by changes in legislation, guidance, technology or school practice.

Implementation Date: November 2026

Review Date: November 2027