ICT and Internet Acceptable Use Policy

Meanwood Church of England Primary School

Approved by:	Board of Governors	**Date:** 1.09.26
Last reviewed on:	1.09.26	
Next review due by:	1.09.27	

Vision and Values

Open Hearts | Open Minds | Open Arms
Our vision is to enrich the lives of our children emotionally, physically, spiritually and academically, where every person is valued, nurtured and empowered. Our vision is underpinned by Jesus' commandment to "love one another as I have loved you" (John 15:12).

This school is committed to safeguarding and promoting the wellbeing of children and young people and expects all staff and volunteers to share this commitment. At Meanwood C of E Primary School we will continuously strive to ensure that everyone in our school is treated with respect and dignity. Each person in our school will be given fair and equal opportunities to develop their full potential with positive regard to gender, ethnicity, cultural and religious background, faith, sexuality or disability. The school will provide an inclusive curriculum, which will meet the needs of all its pupils including those with disabilities, special educational needs, from all cultural backgrounds and faiths and pupils with English as an additional language.

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 senior leadership teams), governors, volunteers and visitors. However, the ICT resources and facilities our school uses also pose risks to data protection, online safety and safeguarding. 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 disciplinary policy.

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.

2. Relevant legislation and guidance

This policy refers to, and complies with, the following legislation and statutory guidance:

- Keeping Children Safe in Education (KCSIE) 2026 (Statutory Guidance)
- Children's Wellbeing and Schools Act 2026 (Statutory Guidance)
- Mobile Phones in Schools (Statutory Guidance, June 2026)
- Data Protection Act 2018 and the UK General Data Protection Regulation (UK GDPR)
- Computer Misuse Act 1990

- Human Rights Act 1998
- The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000
- Education Act 2011 & Education Act 1996
- Freedom of Information Act 2000
- The Education and Inspections Act 2006
- Searching, screening and confiscation: advice for schools (DfE)
- National Cyber Security Centre (NCSC) Guidelines
- Education and Training (Welfare of Children Act) 2021

3. 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 (including Next Generation and Janine Docherty).

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.

4. 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. Unacceptable use 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 (also known as youth-produced sexual imagery or sexting).
- 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 personal device to the school's secure ICT network without explicit approval from authorised personnel.
- Connecting any personal device to the school's ICT network to take images of children without prior written authorisation.
- Setting up any software, applications or web services on the school's network without approval, or using software designed to interfere with network functioning.
- Gaining, or attempting to gain, access to restricted areas of the network without approval.
- Using websites or mechanisms to bypass the school's filtering and monitoring mechanisms.
- Engaging in content or conduct that is radicalised, extremist, racist, anti-Semitic or discriminatory in any other way (violating the Prevent Duty).

This is not an exhaustive list. The school reserves the right to amend this list at any time. The Headteacher will use professional judgement to determine whether any act or behaviour not on the list above is considered unacceptable use.

4.1 Exceptions and Sanctions

Where the use of school ICT facilities (on school premises and/or remotely) is required for a purpose that would otherwise be considered an unacceptable use, exemptions may be granted at the Headteacher's discretion. Requests must be made in writing. Pupils and staff who engage in unacceptable activity face disciplinary action in line with the school's behaviour and staff discipline policies.

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

5.1 Access to school ICT facilities and materials

Next Generation manages access to the school's ICT facilities and materials. Staff will be provided with unique log-in/account information and passwords that they must use. Staff who have access to files they are not authorised to view, or who need their permissions changed, should contact the Headteacher immediately.

5.2 Use of phones and email

The school provides each member of staff with a professional email address, which must be used for all work-related business. Staff must not share their personal email addresses or phone numbers with parents and pupils, and must not conduct work-related business on personal accounts. Staff must use phones provided by the school to conduct work-related communication. Professional email communication must be written with care; emails are disclosable under the Data Protection Act 2018 in legal proceedings. Sensitive or confidential attachments must be encrypted.

5.3 Personal use and social media

Staff are permitted occasional personal use of school ICT facilities, provided it does not take place during teaching hours, takes place when no pupils are present, does not constitute

unacceptable use, and does not interfere with professional duties. Staff may not store personal files (such as personal music, videos, or photos) on school facilities. Staff must ensure their personal use of social media is appropriate, secure, and preserves professional integrity. The PTA Facebook page may only be managed and posted to by authorised personnel. Detailed guidance is provided in Appendix 1 (Facebook Cheat Sheet).

5.4 Statutory Staff Safeguarding Duties (KCSIE 2026 Mandate)

In accordance with the statutory requirements of Keeping Children Safe in Education (KCSIE) 2026, the DfE has removed the condensed Annex A reading pathway for school staff. It is a strict statutory requirement that all school staff members—including governors, contractors, and volunteers in regulated activity—must read Part One of KCSIE 2026 in full. All staff must sign an annual declaration confirming they have read, understood, and will comply with Part One of the guidance. Staff must remain vigilant that safeguarding issues are often interrelated, maintaining an attitude of 'it could happen here'.

5.5 Network Monitoring

The school reserves the right to monitor the use of its ICT facilities and network to ensure compliance with school policies, maintain operational security, and prevent crime. This includes monitoring websites visited, bandwidth usage, school email accounts, school telephone calls, and user activity logs. Monitoring is conducted strictly by authorised personnel to the extent permitted by law.

6. Pupils

6.1 Access to ICT facilities

Pupils have access to computers within the computer suite for curriculum lessons and research. iPads and laptops are provided by the school for educational use in lessons to support curriculum delivery. Pupils must only access these facilities under direct staff supervision.

6.2 Pupil Mobile Phone and Smart Device Policy (Statutory Phone-Free Environment)

To comply with the DfE statutory guidance 'Mobile phones in schools' (effective 1 September 2026) enabled by the Children's Wellbeing and Schools Act 2026, Meanwood C of E Primary School operates a strict 'mobile phone-free by default' environment. Pupils are prohibited from using personal mobile phones, smartwatches with communication/camera capabilities, or any other interactive smart devices throughout the entire school day—including during lessons, the time between lessons, breaktimes, and lunchtimes. Pupils are encouraged to see a phone-free environment as a positive space conducive to focused learning and positive social interaction.

The following procedures must be followed:

- Hand-In: Pupils who bring a personal mobile phone or smart device to school for safety during travel must turn the device off completely before entering the school building.
- Secure Storage: Devices must be handed in to the class teacher immediately upon arrival in the classroom. Staff will place devices in secure, designated storage.

- Dismissal: Devices will be locked away throughout the school day and returned to pupils by the class teacher at dismissal time. Devices must not be turned on until the pupil has left the school building unless specific staff permission is granted.
- Sanctions: Any pupil found in possession of an unhanded personal mobile phone or smart device during the school day will face immediate confiscation of the device, and the parent/carer will be required to collect it from the school office.

6.3 Reasonable Adjustments & Special Circumstances

In accordance with our duties under the Equality Act 2010, the school will make reasonable adjustments to the mobile phone policy for pupils with diagnosed disabilities or complex medical needs. This is managed strictly by exception on a case-by-case basis through a formal individual healthcare plan (IHP) or SEND support plan. For example, a pupil with Type 1 diabetes who requires continuous glucose monitoring (CGM) via a smartphone app will be permitted to have their device. In such cases, the device must remain on the pupil's desk, silent, and be used strictly and exclusively for medical monitoring; any non-medical use (such as web browsing, social media, or messaging) will constitute a breach of this policy and result in disciplinary action.

6.4 Search, Screening, and Confiscation

Under the Education Act 2011 and in line with DfE advice on searching, screening, and confiscation, authorized school staff have the statutory power to search pupils' devices (phones, tablets, computers) if they suspect a breach of school rules or the presence of prohibited material. Authorized staff have the legal right to delete files and data from searched devices if they believe there is 'good reason' (e.g., to prevent teaching disruption or enforce rules). If staff suspect a device contains illegal material, or evidence of abuse, the device will be confiscated immediately and handed to the police. If a staff member suspects a device contains a nude or semi-nude image, they must not view the image but must immediately hand the device to the DSL (Jo Rowlett).

6.5 Unacceptable use of ICT and the internet outside of school

The school will sanction pupils in line with the behaviour policy if they engage in unacceptable use of ICT or the internet outside of school (at any time, even on non-school premises) if it impacts the school community. This includes online bullying or harassment, disparaging the school, sharing confidential school data, or using online spaces to promote extremist or radicalised content (Prevent Duty).

7. Parents

Parents do not have regular access to the school's ICT facilities. Parents working in an official capacity (e.g., volunteers or PTA) may be granted restricted access at the Headteacher's discretion and must abide by the staff acceptable use terms. The school believes in modelling respectful online communication; parents play a vital role in this. Parents are expected to communicate respectfully with and about the school online (via Twitter/X, Teachers2parents, and the school website) and must sign the parent agreement.

8. Data security, Encryption, and WiFi Access

8.1 Passwords and Security Practices

The school is responsible for maintaining network security and user access controls. Users must set strong, unique passwords (at least 8 characters, containing uppercase, lowercase, numbers, and special characters) and keep them confidential. Software updates, firewalls, and anti-virus are automatically configured on all school devices. Users must not circumvent administrative or technical safeguards. School systems, files, and devices have clearly defined access rights managed by Janine Docherty. Users must always lock their laptops (by pressing 'Windows Key + L') when leaving their device and log out completely at the end of the day. Hard drives on school-provided laptops are encrypted to protect data in case of loss or theft.

8.2 School WiFi Networks & Device Separation

To resolve conflicts between network security and classroom device delivery, the school operates a strict network separation policy:

- Secure Educational WiFi: School-provided iPads, laptops, and computer suite terminals used in daily curriculum lessons have exclusive, secure, and monitored access to the school's main administrative and educational WiFi network.
- Pupil WiFi Ban: Pupils are strictly prohibited from connecting personal devices to the school's WiFi networks. Pupil personal devices must not be used to access internet services in school.
- Restricted Guest WiFi: Staff and authorized visitors (who have undergone an enhanced DBS and barred list check) may be permitted to connect personal devices to a separate, restricted, and filtered guest WiFi network, strictly at the Headteacher's discretion. WiFi passwords must never be shared with unauthorized individuals.

9. Protection from cyber attacks (Cyber Essentials 2026)

To protect our network, systems, and data, Meanwood C of E Primary School operates in alignment with the National Cyber Security Centre (NCSC) and the Cyber Essentials 2026 standards. The school implements a multi-layered security framework:

- Annual Audits: The school conducts an annual independent third-party audit to objectively test and verify that cyber controls are proportionate and robust.
- Staff Training: Annual cyber security training is mandatory for all staff (with immediate induction training for mid-year starters), covering sender address verification, phishing detection, payment verification, and reporting protocols.
- Backup Systems: Critical data (including the MIS) is automatically backed up and stored securely in off-site cloud-based backup systems that are completely disconnected from the primary school network.
- Security Infrastructure: Next Generation maintains robust firewalls (always active), anti-virus, automatic patching schedules, and regular access reviews to ensure correct user permissions.

- Ransomware Protocol: In line with NCSC advice, the school will not engage with or pay ransom demands from ransomware attacks, as payment does not guarantee data recovery and encourages criminal activity.
- Incident Response: The school maintains an Incident Response Plan which is tested annually using the NCSC's 'Exercise in a Box'. In the event of a cyber incident, designated staff will immediately activate the plan and notify the statutory agency 'Report Fraud' (formerly Action Fraud).

10. Online safety, active Filtering & Monitoring, and Generative AI

10.1 Strategic Governance & Leadership

Online safety is recognized as a vital safeguarding responsibility. The school operates a collaborative tripartite governance model to oversee digital safety:

- Board of Governors: Holds strategic oversight of the policy, ensures filtering and monitoring systems are appropriate, reviews logs, and conducts an annual review of the school's digital risk profile.
- Headteacher (ICT Manager): Oversees day-to-day technical operations, coordinates with Next Generation to ensure technical security, and acts as the liaison for high-level technical configurations.
- Designated Safeguarding Lead (DSL) Ella Parker: Leads on the safeguarding element of online safety. The DSL manages all online safety safeguarding incidents, maintains the central safeguarding logs, reviews weekly activity reports, and updates and delivers staff training.

10.2 System Reviews (Plan Technology for Your School)

The Board of Governors, Headteacher, and DSL must collaboratively utilize the DfE's 'Plan Technology for Your School' self-assessment tool at least annually. This service evaluates the school's active filtering and monitoring systems, identifies vulnerabilities, and supports the leadership team in implementing necessary upgrades to maintain statutory compliance.

10.3 Defining Modern Digital Risks & Generative AI

The online safety landscape has evolved beyond basic web blocks. The school's filtering and monitoring systems actively target the updated '4 Cs' of online safety, with a specific focus on blocking and flagging:

- Misinformation & Disinformation: Exposure to fake news, manipulated media, and conspiracy theories designed to mislead or cause social harm.
- Generative AI Harms: Risks associated with the misuse of artificial intelligence, including deepfakes, automated plagiarism, and unauthorized processing of personal data.
- Radicalisation & Hate Speech: Extremist content, misogynistic or incel-related material, and online hate speech.

Rules for Generative AI Usage in School:

- Approved Tools Only: Staff and pupils must only use generative AI tools and platforms that have been officially reviewed and approved by the Headteacher and Next Generation, ensuring compliance with DfE product safety expectations.
- Data Protection: Personal data of pupils, staff, or parents must never be entered into generative AI prompts, as this breaches data protection regulations.
- Academic Integrity: Pupils must be taught the ethical boundaries of AI. Using AI to generate coursework or homework and presenting it as their own work is strictly prohibited and will be treated as academic malpractice in line with the behaviour policy.
- Staff Supervision: Pupils' use of generative AI tools must be closely supervised by staff to ensure safety, accuracy, and constructive educational value.

11. Monitoring, review, and related policies

This policy is reviewed annually by the Headteacher and approved by the Board of Governors. It must be read alongside the school's related policies: Child Protection and Safeguarding Policy, Behaviour Policy, Staff Discipline Policy, Data Protection Policy, and the Online Safety Policy.

Appendix 1: Facebook cheat sheet for staff

- Change your display name: Use your first and middle name, a maiden name, or put your surname backwards to make your profile harder to find.
- Change your profile picture: Use an unidentifiable image, or ensure the image is professional and neutral.
- Check privacy settings: Regularly check your settings. Change the visibility of your posts and photos to 'Friends only', rather than 'Friends of friends'.
- Tagging: Be careful about tagging other staff members in images or posts, and ask others to do the same for you.
- Public Posts: Don't share anything publicly that you wouldn't be happy showing your pupils or parents. The public may still see posts you 'liked' on public pages.
- No Pupil Friend Requests: Never accept friend requests from current or former pupils on social media. Ignore and delete the request, block the pupil, and notify SLT if they persist.
- Parent Friend Requests: Avoid accepting friend requests from current parents. Responding to one sets a difficult precedent and may give pupils indirect access to your profile.
- Harassment Protocol: If you are harassed or see offensive material about yourself on social media, do not retaliate. Take screenshots as evidence, report to the platform, and notify the Headteacher immediately.
- No Social Media During Work: Personal social media sites must not be accessed during school hours.
- Work Email Separation: Never link your school email address to your personal social media accounts.

Appendix 2: Glossary of cyber security terminology

Antivirus: Software designed to detect, stop and remove malicious software and viruses.

Cloud: Where you can store and access your resources (including data and software) via the internet, instead of locally on physical devices.

Cyber attack: An attempt to access, damage or disrupt your computer systems, networks or devices maliciously.

Cyber incident: Where the security of your system or service has been breached.

Cyber security: The protection of your devices, services and networks (and the information they contain) from theft or damage.

Firewall: Hardware or software that uses a defined rule set to constrain network traffic – this is to prevent unauthorised access.

Malware: Malicious software. This includes viruses, trojans or any code or content that can adversely impact individuals or organisations.

Phishing: Untargeted, mass emails sent to many people asking for sensitive information (like bank details) or encouraging them to visit a fake website.

Ransomware: Malicious software that stops you from using your data or systems until you make a payment.

Two-factor/multi-factor authentication: Using 2 or more different components to verify a user's identity.