Life in all its fullness

learning together, inspiring each other, achieving our best

Marshfield CE VC Primary School

# IT, Digital Infrastructure & Social Media Acceptable Use Policy (AUP)

# Statutory Safeguarding & Online Safety Framework (2026/27)

| | |
|---|---|
| **Statutory Status & Framework** | Statutory Guidance — DfE Keeping Children Safe in Education (KCSIE 2026), Data (Use and Access) Act 2025, Education Act 2002 (s175), Crime and Policing Act 2026 |
| **School Vision & Values** | Marshfield CE VC Primary School — 'Learning Together, Inspiring Each Other, Achieving Our Best' |
| **Key Safeguarding Contacts** | Headteacher & DSL: Jessica Bolt \| Chair of Governors: Hugh Campbell \| Safeguarding Governor: Emma Bradley |
| **Technical & IT Leadership** | IT Managed Service Provider (Integra) & Online Safety Lead / Deputy DSLs |
| **Target Audience & Scope** | All Staff, Governors, Volunteers, Contractors, External Tutors, Visitors, Pupils, and Parents |
| **Approval & Review Cycle** | Approved by Governing Board: October 2026 \| Next Annual Review: October 2027 |

## 1. Policy Statement, Ethos & Statutory Framework

Marshfield CE VC Primary School is fully committed to leveraging digital technology, educational software, and online resources to enrich learning while establishing robust safeguards against digital harm. In accordance with Department for Education (DfE) statutory guidance **Keeping Children Safe in Education (KCSIE 2026)**, online safety is recognised as an integral, non-negotiable component of the school's overarching safeguarding duty. The school operates an 'it can happen here' ethos, maintaining constant vigilance regarding online risks, cyberbullying, grooming, exposure to illegal or harmful content, data breaches, and emerging technologies including generative Artificial Intelligence (AI).

This policy outlines the acceptable and unacceptable uses of school IT infrastructure, internet access, email, mobile devices, digital imagery, and social media platforms. It applies to all adults working with children within our school community—including paid staff, governors, supply teachers, student teachers, volunteers, contractors, and visitors—as well as to pupils and parents. Compliance with this policy is mandatory and forms an explicit condition of employment and appointment.

## 2. Governance, Leadership & Individual Responsibilities

Effective digital safeguarding requires clear leadership, continuous oversight, and shared accountability across the entire school community:

- **The Governing Board:** Under the leadership of Chair Hugh Campbell and Safeguarding Governor Emma Bradley, the Governing Board maintains strategic oversight of IT safety, ensuring compliance with DfE Filtering and Monitoring Standards, reviewing annual online safety audits, and evaluating policy effectiveness.
- **The Headteacher & Designated Safeguarding Lead (DSL):** Jessica Bolt holds overall operational responsibility for online safety and digital safeguarding. The DSL ensures prompt intervention in response to online safety concerns, coordinates with South Gloucestershire Children's Partnership, and ensures all staff receive annual online safety training.
- **IT Managed Service Provider & Technical Leads:** Responsible for maintaining secure technical architecture, implementing resilient age-appropriate web filtering (NCSC/UKSaferInternet accredited), configuring automated keyword monitoring, ensuring endpoint protection/antivirus updates, and managing user access permissions.
- **All Staff & Adult Community Members:** Must model exemplary digital professionalism, protect pupil data under the Data (Use and Access) Act 2025, adhere to filtering rules, strictly enforce device policies, and report digital safety concerns or system vulnerabilities immediately.

## 3. Acceptable Use of School Network, Hardware & Infrastructure

School network accounts, hardware (laptops, iPads, desktop PCs), cloud storage platforms (Google Workspace / Microsoft 365), and email systems are provided strictly for educational and administrative purposes:

### 3.1 Password Hygiene, Authentication & Account Security

Staff must maintain complex passwords (minimum 12 characters combining letters, numbers, and symbols) and utilize Multi-Factor Authentication (MFA) where enabled. User credentials must never be shared, written down, or stored in plaintext. Staff must lock their screen (Windows Key + L or Mac equivalent) whenever stepping away from a terminal, even for seconds.

### 3.2 Network Integrity & Unauthorised Hardware/Software

Staff, volunteers, and visitors are strictly prohibited from connecting non-approved personal hardware (such as personal laptops, router equipment, or unvetted USB storage drives) to the secure internal curriculum or administrative network without authorisation from the Headteacher. Downloading or installing unauthorized executable software, games, or browser extensions is strictly forbidden.

### 3.3 Incidental Personal Use

Incidental personal use of school internet and email by staff is permitted during non-directed time (e.g. lunch breaks), provided it does not interfere with professional duties, consume excessive network bandwidth, involve commercial/financial activity, or violate any safeguarding standard.

## 4. Filtering, Monitoring & Cyber Security Standards

In full compliance with DfE Technical Standards for Schools and KCSIE 2026, Marshfield Primary School enforces active web filtering and automated monitoring to protect pupils and staff from harmful content:

### 4.1 Filtering Architecture & Prohibited Content Categories

The school's Internet Service Provider (ISP) and endpoint filtering system block access to illegal content (including CSAM and terrorist materials), adult/pornographic content, gambling, extremist views, violence, illegal drug procurement, and unmoderated social networks. Circumventing filtering via Virtual Private Networks (VPNs), proxy websites, or cellular hotspots is a major disciplinary violation.

### 4.2 Staff Duty to Report Over-blocking and Under-blocking

Staff must actively monitor filtering performance during classroom instruction. If a legitimate educational site is blocked ('over-blocking'), staff should submit a request to the IT Managed Service Provider. If inappropriate content bypasses the filter ('under-blocking'), staff must immediately isolate the device, protect pupils from viewing the content, and report the URL directly to the DSL and IT Lead.

### 4.3 Cyber Security & Data Protection (Data (Use and Access) Act 2025)

All personal data regarding pupils, families, and personnel must be stored strictly within encrypted, school-approved cloud storage environments. Transporting unencrypted pupil data on removable media (USB drives) is strictly banned. Staff must remain vigilant against phishing, email spoofing, and social engineering attacks, immediately reporting suspicious emails to the IT Helpdesk.

## 5. Mobile Phones, Smart Devices & Personal Technology

To eliminate distraction, protect pupil privacy, and maintain a safe learning environment, Marshfield Primary School enforces clear rules regarding personal electronic devices:

**MANDATORY POLICY: CLASSROOM MOBILE-PHONE FREE DEFAULT**

1. Staff Personal Mobile Devices: Must be switched off or placed in silent mode and stored securely in lockers or staffroom storage during directed hours. Personal phones must NEVER be visible or used in classrooms, corridors, or playground duty areas when children are present.
2. Photography & Recording Prohibition: Personal mobile phones or personal cameras must NEVER be used to photograph, record, or film pupils under any circumstances.
3. Smartwatches & Wearable Tech: Smartwatches with internet, messaging, or camera capabilities must have cellular/camera functions disabled during classroom instruction and assessment conditions.
4. Pupil Mobile Devices: Pupils are strongly discouraged from bringing mobile phones to school. Where a Year 5/6 pupil requires a phone for safety when walking home independently, the phone must be handed to the school office upon arrival, stored securely, and collected at home time.

## 6. Social Media & Online Professional Boundaries

The boundary between professional life and personal social media use must be rigorously maintained to protect pupils and preserve public confidence in the school:

### 6.1 Interactions with Pupils and Parents

Staff, volunteers, and contractors must **NEVER** accept 'friend requests', follow, send direct messages to, or engage in social media interactions with current pupils or former pupils under 18 years of age across any personal social network (e.g. Facebook, Instagram, TikTok, Snapchat, X, WhatsApp). Personal communications

with parents via personal social media or personal messaging apps regarding school matters is strictly prohibited; all communication must go through official school communication channels.

### 6.2 Professional Conduct & School Reputation

Staff must ensure that their personal social media accounts are configured with high privacy settings. Staff must not publish content, commentary, or media that brings Marshfield Primary School into disrepute, compromises professional confidentiality, discloses pupil information, or contains derogatory comments regarding pupils, families, or colleagues.

### 6.3 Official School Social Media Channels

Official school social media accounts (e.g. school X/Twitter or Facebook page) are managed exclusively by designated authorised administrators under the direct supervision of the Headteacher. Posts must showcase learning achievements, refrain from publishing identifiable pupil full names alongside photos, and adhere strictly to parental media consent records.

## 7. Photography, Visual Media & Digital Asset Management

Images and video footage of pupils constitute personal data under the Data (Use and Access) Act 2025 and require strict governance:

- **School-Issued Cameras & Tablets Only:** All photographs and recordings of pupils must be captured using school-owned digital cameras or school iPads. Under no circumstances may staff use personal smartphones, personal tablets, or personal cameras.
- **Parental Consent Register:** Prior to taking or publishing any image, staff must verify parental consent preferences on the school management information system (MIS). Images of pupils whose parents have opted out of media publication must not be used on websites, newsletters, or social media.
- **Secure Asset Transfer & Storage:** Digital photos must be transferred directly from school devices to the secure, access-controlled school cloud network and deleted from local device memory. Images must never be stored on personal computers or external unencrypted drives.

## 8. Generative AI & Emerging Educational Technologies

Marshfield Primary School recognises the potential educational benefits of Artificial Intelligence (AI) tools while enforcing clear safeguards regarding data privacy, intellectual property, and academic integrity:

- **Protection of Personal & Special Category Data:** Staff must NEVER enter pupil personal data (full names, dates of birth, EHCP details, safeguarding notes, or assessment records) into public generative AI platforms (e.g. ChatGPT, Claude, Gemini, Copilot). Doing so constitutes an illegal data transfer under the Data (Use and Access) Act 2025.
- **Pedagogical Integrity & Verification:** AI tools used for lesson planning or resource drafting must be critically reviewed for factual accuracy, age-appropriateness, and bias before classroom deployment. Staff remain fully responsible for the content delivered to pupils.
- **Awareness of AI Deepfakes & Synthetic Media:** Staff must remain alert to the risks of synthetic image generation, voice cloning, and AI deepfakes used for cyberbullying, impersonation, or harassment. Any discovery or suspicion of synthetic media created to target pupils or staff must be immediately reported to the DSL as a serious safeguarding incident.

## 9. Incident Management, Reporting & Misuse Sanctions

Digital safety breaches or policy violations are managed through structured reporting pathways depending on the nature and severity of the incident:

| Breach Category | Example Scenarios | Action & Escalation Pathway |
|---|---|---|
| Minor / Accidental Misuse | Accidental visit to an inappropriate pop-up site; unintentional password slip; leaving a terminal unlocked in a secure staff room. | Log with IT Lead; internal review; password reset; refresher guidance on digital hygiene. |
| Low-Level Concern / Policy Violation | Using personal mobile phone in a corridor; friending a parent on personal social media; minor inappropriate comment online; inputting non-sensitive work data into unapproved AI. | Reported to DSL/Headteacher within 24 hours under Low-Level Concerns Policy; documented on confidential LLC log; line management discussion. |
| Major Safeguarding / Data Breach / Gross Misconduct | Accessing/sharing illegal content; taking photos of pupils on personal devices; cyberbullying/harassment; sharing pupil confidential data externally; deliberate filtering bypass. | Immediate disconnection from network; suspension of IT privileges; investigation under Disciplinary Policy; referral to LADO within 1 working day; DBS/TRA statutory referral; police notification if criminal. |

## 10. Appendix A: Staff & Governor Acceptable Use Agreement

All staff, governors, volunteers, and contractors must complete and return this declaration prior to being granted access to school IT systems:

| | |
|---|---|
| **Full Name of Staff / Adult:** | |
| **Role / Job Title:** | |
| **Type of Worker:** | Staff [ ] Governor [ ] Volunteer [ ] Contractor [ ] |
| **Confirmation of Reading:** | I confirm that I have read, understood, and agree to abide by the Marshfield Primary School IT & Social Media Acceptable Use Policy (2026/27). |
| **Key Commitments:** | I agree to:<br>• Protect passwords and lock terminals when away.<br>• Keep personal mobile devices off/stored away during directed time.<br>• Never use personal devices to photograph pupils.<br>• Maintain strict online professional boundaries with pupils and parents.<br>• Adhere to filtering/monitoring rules and report all digital safety concerns. |

| | |
|---|---|
| **Signature & Date:** | Signature: _____ Date: ____/____/2026 |

## 11. Appendix B: Pupil Acceptable Use Rules (KS1 & KS2)

### 11.1 Key Stage 1 (Reception, Year 1 & Year 2) - Digital Code

- I only use school computers and iPads when an adult tells me to.
- I keep my passwords secret.
- I tell a teacher or adult straight away if I see something online that makes me feel sad, scared, or confused.
- I am kind and gentle when using school devices.

### 11.2 Key Stage 2 (Years 3, 4, 5 & 6) - Digital Agreement

- I will only use the internet and school devices for schoolwork and when a teacher gives permission.
- I will keep my logins and passwords safe and never share them with classmates.
- I will always be polite, respectful, and kind when writing messages or working online.
- I will never look for, save, or send anything that could upset or hurt others.
- If I see something online that worries me or seems unsafe, I will report it to a teacher immediately.
- I understand that the school checks the websites I visit to keep me safe.