Life in all its fullness

learning together, inspiring each other, achieving our best

Marshfield CE VC Primary School

DATA PROTECTION & ONLINE SAFETY POLICY

Statutory Policy Framework Incorporating DfE Filtering & Monitoring Standards, KCSIE 2026, UK GDPR, Data (Use and Access) Act 2025, and Cyber Security Guidelines

Policy Attribute	Policy Specification & School Governance Details
Statutory Framework	KCSIE 2026 | UK GDPR & Data Protection Act 2018 | Data (Use and Access) Act 2025 | DfE Filtering & Monitoring Standards | Education Act 2002 (s175)
Ratification & Review	Ratified by Governing Body: October 2026 | Due for Review: October 2027 (Annual Review)
Key Safeguarding Contacts	Headteacher & DSL: Jessica Bolt Chair of Governors: Hugh Campbell | Safeguarding Governor: Emma Bradley Deputy DSLs: Phillippa Tilley & Tomi Looker-Jones
Technical & IT Support	Integra Schools IT / South Gloucestershire Technical Team (Service Desk: 01454 863838) Filtering Provider: iBoss Active Monitoring & Filtering Solution

1. Policy Statement & Statutory Legal Framework

Marshfield CE VC Primary School is fully committed to creating a secure, transparent, and safe digital environment for all pupils, staff, governors, and visitors. In accordance with our core ethos—'Learning Together, Inspiring Each Other, Achieving Our Best'—the school recognises that modern information and communications technology (ICT), digital learning platforms, and online networks offer immense educational benefits, while simultaneously introducing complex safeguarding, privacy, and technical risks.

This Data Protection & Online Safety Policy establishes an integrated statutory framework governing the safe, lawful, and ethical use of technology, personal data management, and digital communications across the school community. It operates on the fundamental principle that online safety is an interwoven, whole-school safeguarding responsibility underpinned by an uncompromising 'it can happen here' culture.

> **STATUTORY DATA PROTECTION & SAFEGUARDING OVERRIDE (KCSIE 2026 & DUA ACT 2025)**
> Data protection legislation—including the UK GDPR, Data Protection Act 2018, and Data (Use and Access) Act 2025—DOES NOT prevent or inhibit the sharing of personal or special category information for the purposes of keeping children safe and promoting their welfare. Under KCSIE 2026 (Part 2, para 147-148), fears about sharing information must NEVER be allowed to stand in the way of safeguarding children. 'Safeguarding of children and individuals at risk' is an explicit processing condition under data protection law that allows practitioners to store and share special category personal data without consent where seeking consent would place a child at risk of harm or prejudice an investigation.

1.1 Statutory Legislation and National Guidance

This policy directly incorporates and complies with the following statutory requirements and national standards:

- Keeping Children Safe in Education (KCSIE 2026) — Statutory guidance from the Department for Education (DfE) under Section 175 of the Education Act 2002.
- Data (Use and Access) Act 2025 & Data Protection Act 2018 / UK General Data Protection Regulation (UK GDPR) — Establishing statutory rules for processing, storing, and sharing personal data.
- DfE Filtering and Monitoring Standards for Schools and Colleges (2026) — Mandatory technical and governance requirements for limiting exposure to online harms.
- DfE Cyber Security Standards for Schools and Colleges — Operational benchmarks for technical resilience, access management, and incident response.
- Working Together to Safeguard Children 2026 — Multi-agency safeguarding framework and early help assessment protocols.
- Human Rights Act 1998 & Equality Act 2010 (including the Public Sector Equality Duty) — Protecting fundamental rights and preventing discriminatory harm.
- Crime and Policing Act 2026 & Safeguarding Vulnerable Groups Act 2006 — Regulated activity standards and statutory barred list requirements.
- DfE Statutory Guidance on Mobile Phones in Schools — Establishing mobile phone-free school environments by default.
- DfE Guidance on Generative Artificial Intelligence in Education (2026) — Risk management, data protection, and intellectual property standards.

2. Governance, Roles & Responsibilities

Effective data protection and online safety require a coordinated approach involving all levels of school leadership, technical staff, educators, pupils, and parents. Specific roles and accountabilities are defined as follows:

2.1 The Governing Body & Safeguarding Governor

The Governing Body (led by Chair Hugh Campbell and Safeguarding Governor Emma Bradley) holds strategic oversight for digital safety, information governance, and filtering systems:

- Ensures that the school complies with data protection laws, KCSIE 2026, and DfE Technical Standards.
- Receives and reviews an Annual Filtering & Monitoring Assurance Report presented by the Headteacher and Technical Lead.
- Ensures all governors receive appropriate safeguarding and online safety training at induction and regular annual updates.
- Approves and annually reviews this policy, ensuring it is publicly accessible on the school website.

2.2 Headteacher & Designated Safeguarding Lead (DSL)

Headteacher Jessica Bolt acts as the overall lead for safeguarding and online safety, supported by Deputy DSLs Phillippa Tilley and Tomi Looker-Jones:

- Holds strategic responsibility for integrating online safety into the whole-school safeguarding framework.
- Overcomes 'over-blocking' issues by managing site unblocking requests to ensure the curriculum remains rich and unrestricted for safe educational content.

- Maintains oversight of filtering logs, active monitoring alerts (iBoss), and digital incident reporting.
- Acts as Senior Information Risk Owner (SIRO), ensuring robust management of personal data and security risk registers.
- Ensures robust cover arrangements (including a confidential shared safeguarding mailbox: safeguarding@marshfieldprimary.org.uk) so safeguarding and online alerts are monitored without delay.

2.3 Strategic IT Lead & Technical Support Provider (Integra)

Technical support is delivered in partnership with Integra Schools IT (Service Desk: 01454 863838):

- Maintains secure network infrastructure, firewalls, wireless security, and endpoint protection across all school devices.
- Deploys and manages the iBoss active network filtering and monitoring solution, ensuring daily updates against IWF CAIC lists and police-assessed unlawful content lists.
- Enforces password policies, user access rights, secure data backups, and technical cyber-security patches.
- Ensures administrator credentials are restricted and securely held off-site by the Local Authority technical team.

2.4 Teaching & Support Staff

- Undergo annual online safety and filtering/monitoring training as part of mandatory safeguarding CPD.
- Embed online safety, digital literacy, and critical thinking across the PSHE, Computing, and wider curriculum.
- Pre-screen websites and digital resources prior to classroom presentation.
- Enforce acceptable use rules and report any technical vulnerabilities, accidental exposure to inappropriate content, or pupil digital distress immediately to the DSL.
- Ensure no personal devices (mobile phones, smartwatches) are used in classrooms or pupil areas during directed hours.

2.5 Parents, Carers & Pupils

- Pupils learn age-appropriate digital resilience, follow the Pupil Acceptable Use Policy (AUP), and report online concerns to trusted adults.
- Parents endorse the Pupil AUP, support safe internet habits at home, and adhere to school guidelines regarding mobile devices and digital photography at school events.

3. DfE Filtering & Monitoring Standards & Technical Provisions

In compliance with KCSIE 2026 (paragraphs 173–177) and the DfE Filtering and Monitoring Standards, Marshfield Primary School implements robust technical measures to block harmful material and actively monitor digital activity across all school-owned devices, networks, and internet connections.

3.1 Filtering System Architecture

Internet access across the school is managed via the South Gloucestershire Integra IT network, utilising the iBoss filtering and active threat protection architecture. Filtering operates at the network level and does not rely on device-side client software that could be bypassed or disabled by users.

- Automated Block Lists: Actively blocks Child Sexual Abuse Material (CSAM) using the Internet Watch Foundation (IWF) CAIC list, and unlawful terrorist content using Home Office police-assessed lists.

- Categorised Content Blocking: Automatically blocks access to adult content, extreme violence, radicalisation, self-harm/suicide encouragement, illegal gambling, cybercrime tools, and unverified generative AI applications.
- Differentiated Filtering Profiles: Implements tailored profiles for staff and pupils to prevent 'over-blocking' from restricting age-appropriate teaching on sensitive RSHE topics (e.g. puberty, online harms, domestic safety).
- Unblocking Requests: Staff requests to unblock educational websites must be submitted formally to the Headteacher/DSL for approval before technical configuration by Integra IT.

3.2 Active Monitoring & Automated Alert Escalation

The school employs a hybrid monitoring strategy combining active automated threat detection with human oversight:

- Real-Time Keyword & Behaviour Alerts: The iBoss system monitors search terms, web activity, and network communications for concerning language or behavioral indicators (e.g. suicide ideation, grooming terms, weapons, radicalisation).
- Multi-Recipient Incident Alerts: Automated alert notifications are delivered simultaneously to Headteacher Jessica Bolt, Deputy DSLs, and Integra IT support to ensure monitoring does not rely on a single individual.
- Proactive Technical Oversight: External technical support (Integra) assists the school by flagging anomalous network traffic, surge activity, or severe risk indicators.
- Annual Filtering Review: The DSL and IT Lead conduct an annual formal self-assessment using the DfE 'Plan Technology for Your School' service and present an assurance audit to the Governing Body in Term 6.

4. Data Protection, Cyber Security & Information Governance

Under the Data (Use and Access) Act 2025 and UK GDPR, Marshfield Primary School operates as a registered Data Controller with the Information Commissioner’s Office (ICO). The school enforces strict technical and organisational measures to ensure personal data is processed lawfully, fairly, transparently, and securely.

4.1 Principles of Data Processing

All personal data held by the school must be:

- Processed lawfully, fairly, and in a transparent manner in relation to the data subject.
- Collected for specified, explicit, and legitimate educational and safeguarding purposes.
- Adequate, relevant, and limited to what is necessary in relation to the purposes for which it is processed.
- Accurate and kept up to date; inaccurate data is erased or rectified without delay.
- Kept in a form which permits identification of data subjects for no longer than is necessary.
- Processed securely using appropriate technical (encryption, password controls) and organisational measures.

4.2 Processing Special Category Personal Data & Safeguarding Conditions

Special category data (including medical records, ethnicity, SEND information, and child protection files) receives enhanced legal protection. The school relies on statutory processing conditions under Article 9 of UK GDPR and Schedule 1 of the Data Protection Act 2018:

- Statutory Condition: Processing is necessary for reasons of substantial public interest, specifically 'Safeguarding of children and individuals at risk'.
- Consent Exception: Consent is NOT required to process or share special category data for safeguarding purposes where obtaining consent would place a child at risk or compromise statutory duties.

4.3 Subject Access Requests (SARs) & Serious Harm Test

Data subjects (parents/carers and pupils) have the right to request access to personal data held about them. However, in accordance with Section 146 of KCSIE 2026 and Data Protection Regulations:

> **THE SERIOUS HARM TEST & WITHHOLDING SAFEGUARDING DATA**
> The school MUST NOT disclose personal data in response to a Subject Access Request (SAR) where the 'Serious Harm Test' under data protection law is met. For example, where disclosing information would reveal the location of a child in a refuge or emergency accommodation, or where disclosure would expose a child to a risk of serious physical or mental harm or compromise a child protection investigation, the data MUST be withheld. Independent legal advice will be sought in cases of doubt.

4.4 Secure Transfer of Child Protection Files

When a pupil transfers to another educational institution (in-year or at transition):

- The Child Protection file MUST be transferred to the receiving school as soon as possible, and strictly within 5 working days for in-year transfers or within the first 5 days of a new term.
- Transit must be executed securely via encrypted file transfer (e.g. CPOMS secure transfer) or registered mail. Confirmation of receipt must be obtained and logged.
- The CP file MUST be maintained separately from the pupil's general educational record.
- The exporting DSL must provide a clear structured summary distinguishing current safeguarding risks from historic contextual background.

4.5 Cyber Security Standards & Document Retention

In alignment with DfE Cyber Security Standards:

- Password & Access Controls: All school systems require unique individual user logins with multi-factor authentication (MFA) for remote management access. Shared or generic logins are strictly prohibited.
- Removable Media & Encryption: Staff must NOT store unencrypted pupil personal data on personal USB flash drives or unencrypted external hard drives. Cloud storage (Microsoft 365 / OneDrive) is mandatory.
- Retention of DBS Certificates: Copies of DBS certificates and criminal record disclosures are destroyed securely within 6 months of recruitment, in compliance with UK GDPR Article 10. The Single Central Record (SCR) retains permanent verification details.
- Data Disposal: Paper records containing personal data must be cross-cut shredded on site. Electronic hardware must be securely wiped and certified by an accredited Local Authority disposal partner.

5. Curriculum, Preventative Education & Generative AI

Educating pupils to navigate the online world safely, critically, and ethically is a core statutory duty. Online safety is embedded progressively across Key Stage 1 and 2 within Computing, PSHE, and RSHE lessons, utilizing the SWGfL Digital Literacy and South Gloucestershire frameworks.

5.1 The Four Cs of Online Risk

Curriculum coverage and risk management are structured around the four statutory risk categories (KCSIE 2026):

- Content: Being exposed to illegal, harmful, or age-inappropriate content (e.g. pornography, extreme violence, radicalisation, self-harm, misinformation/disinformation, and fake news).
- Contact: Experiencing harmful online interactions (e.g. peer pressure, grooming, contact with strangers, commercial exploitation, or adult impersonation).
- Conduct: Engaging in personal online behavior that causes harm (e.g. cyberbullying, non-consensual sharing of images, or sending abusive messages).
- Commerce: Exposure to financial exploitation, online gambling risks, commercial scams, or phishing attempts.

5.2 Generative Artificial Intelligence (AI) Safeguards

In accordance with DfE Guidance on Generative AI in Education (2026), Marshfield Primary School recognises both the educational opportunities and significant safeguarding/data risks associated with AI tools:

- Data Protection: Staff and pupils must NEVER enter personal data, special category data, or identifiable pupil work into public Generative AI platforms (e.g. ChatGPT, Claude, Midjourney), as data inputted may be ingested into training models.
- AI-Generated Imagery & Deepfakes: Staff receive explicit training on detecting and responding to AI-generated nudes, 'nudification' applications, and deepfakes. AI-generated sexual imagery of children is treated legally and procedurally as illegal Child Sexual Abuse Material (CSAM).
- Plagiarism & Critical Evaluation: Pupils are taught to critically evaluate AI-generated outputs for bias, hallucination, and factual inaccuracy, upholding academic integrity.

5.3 Mobile Phone-Free School Environment

Marshfield Primary School operates as a mobile phone-free environment by default during the school day. Pupils are prohibited from possessing or accessing personal mobile phones or smartwatches during lessons, breaktimes, or lunchtime. Any permitted exceptional devices (e.g. Year 5/6 pupils walking home independently) must be powered off and surrendered to the school office upon arrival.

6. Managing Online Safety Incidents & Child-on-Child Harm

Online safety incidents (including cyberbullying, online sexual harassment, image sharing, and digital extortion) are managed strictly as safeguarding concerns under the school’s Safeguarding and Child Protection Policy.

6.1 Handling Nudes and Semi-Nudes (Consensual & Non-Consensual)

When responding to incidents involving nude or semi-nude imagery (including AI-generated content), staff must follow UKCIS statutory guidance:

- Immediate Isolation & Support: Support the child in a calm, non-judgmental manner. Reassure the victim that they are not in trouble.
- STRICT PROHIBITION ON VIEWING / FORWARDING: Staff MUST NOT view, download, print, or forward illegal images of a child on any device. Forwarding or copying constitutes a severe criminal offence. Devices containing imagery must be confiscated, secured, and handed to the Police/DSL.

- Takedown Protocols: Utilize the Childline / IWF 'Report Remove' tool to assist children in securing the removal of shared images from public online platforms.
- Proportionate Safeguarding Response: Differentiate between consensual sharing between peers of similar age and coercive/exploitative distribution, applying appropriate pastoral support, parental engagement, and police escalation.

6.2 Cyberbullying & Online Extortion

- Cyberbullying incidents taking place on or off school premises that impact pupil welfare at school are investigated under the Behaviour and Safeguarding Policies.
- Financially Motivated Sexual Extortion (FMSE): Incidents involving online blackmail or extortion must be reported immediately to the Police (101) and CEOP Safety Centre.

6.3 Alignment with Low-Level Concerns & Whistleblowing

- Concerns regarding adult online behavior, improper staff-pupil digital contact, or personal social media breaches must be reported to Headteacher Jessica Bolt under the Low-Level Concerns Policy within 24 hours.
- Where internal safeguarding failures or suppression of online safety breaches occur, staff must escalate via the Whistleblowing Policy to the LADO or NSPCC Whistleblowing Helpline (0800 028 0285).

7. Use of Digital Images, Video & Social Media Governance

7.1 Pupil Photography & Media Consent

- Written parental consent is obtained upon admission for taking and using digital images/videos of pupils.
- Full pupil names are NEVER published alongside photographs on the school website, newsletter, or official social media channels.
- Photos must only be taken on school-owned cameras or iPads; staff are strictly forbidden from using personal mobile devices to photograph pupils.

7.2 Parent Photography at School Events

- In accordance with Information Commissioner’s Office (ICO) guidelines, parents/carers are permitted to capture digital images/videos at school plays, sports days, and assemblies for personal family use.
- To respect child privacy and safeguarding, parents MUST NOT upload or publish photographs/videos containing images of other children onto personal social media accounts.

7.3 Official & Personal Social Media Conduct

- Official Channels: The school website and official social media feeds (Twitter/Facebook) are managed exclusively by named designated staff. Content is pre-approved by the Headteacher.
- Staff Personal Social Media: Staff must maintain strict professional boundaries. Staff must not accept current pupils or parents as 'friends' or contacts on personal social media profiles, and must never discuss school business, pupils, or colleagues online.

8. Incident Escalation Pathway & Key Agency Contacts

In the event of an online safety, data protection, or digital safeguarding incident, the following escalation pathways apply:

Agency / Authority	Role / Scope of Support	Contact Details
Headteacher & DSL	Internal School Lead for Safeguarding & Online Safety	Jessica Bolt — 01225 891246 /
South Glos Access & Response Team (ART)	Children's Social Care Referrals & Urgent Child Protection	Phone: 01454 866000 (Mon-Fri) / 01454 615165 (Out of Hours)
Local Authority Designated Officer (LADO)	Allegations against Staff, Volunteers, or Contractors	LADO Team — 01454 868508 / lado@southglos.gov.uk
Integra Schools IT Service Desk	Technical Support, Filtering Adjustments & Cyber Security	Service Desk: 01454 863838 / IntegraIT@southglos.gov.uk
Professional Online Safety Helpline	Dedicated Advice Line for School Staff & DSLs	Phone: 0344 381 4772 / helpline@saferinternet.org.uk
CEOP Safety Centre (NCA)	Reporting Child Sexual Abuse, Grooming & Exploitation	Online Reporting Portal: https://www.ceop.police.uk/ceop-reporting/
NSPCC Whistleblowing Helpline	External Escalation for Safeguarding Practice Failures	Phone: 0800 028 0285 / help@nspcc.org.uk

Appendix A: Annual Staff & Volunteer Data Protection & Online Safety Declaration

All adults working with or alongside children at Marshfield CE VC Primary School are required to sign and return this declaration upon appointment and following annual review in Term 1.

Member of Staff / Volunteer Name:	
Role / Job Title:	
Declaration Statement:	I confirm that I have read, understood, and agree to abide by the Marshfield CE VC Primary School Data Protection & Online Safety Policy (2026/27), Staff Code of Conduct, and Acceptable Use Policy. I understand my statutory duties regarding filtering and monitoring, data privacy, and safeguarding information sharing.
Signature:	
Date Signed:	
Counter-Signature (Headteacher / DSL):	