Spring Bank Primary School

Online Safety Policy
September 2026

Headteacher: Jordan License
Designated Safeguarding Lead (DSL): Jordan License
Online Safety Coordinator: Tracey Baruah
Online Safety Governor: Lee Arnell
ICT Management Partner / Technical Provider: Datacable
Filtering & Monitoring Software Provider: Classroom Cloud

1. Policy Statement and Aims

At Spring Bank Primary School, we recognise that digital technology and the internet are integral elements of 21st-century education and everyday life. Our mission is to deliver an outstanding, safe, and empowering education at the heart of our community. As part of our statutory safeguarding duty, Spring Bank Primary School is required to ensure that children and young people are protected, educated, and supported when using digital technologies both in school and in the wider world.
This policy aims to:

- Provide robust, proactive processes to ensure the online safety of pupils, staff, volunteers, and governors.
- Identify and support groups of pupils who may be at greater risk of harm online (including

vulnerable children, victims of abuse, and pupils with Special Educational Needs and/or Disabilities [SEND]).
- Deliver an effective approach to online safety, empowering the whole school community to use technology safely and responsibly.
- Establish clear mechanisms to identify, intervene in, log, and escalate online safety incidents and concerns.
- Ensure full alignment with statutory guidance including *Keeping Children Safe in Education (KCSIE) 2026*, Working Together to Safeguard Children, and relevant DfE standards.

2. Statutory Framework and Legislation

This policy is based on statutory guidance and national legislation, including but not limited to:

- DfE statutory guidance: *Keeping Children Safe in Education (KCSIE) 2026*
- DfE guidance: *Teaching Online Safety in Schools*, *Meeting Digital and Technology Standards in Schools*, *Preventing and Tackling Bullying*, and *Mobile Phones in Schools*
- Education Act 1996, Education and Inspections Act 2006, Education Act 2011, and Children's Wellbeing and Schools Act 2026
- Equality Act 2010 and Data Protection Legislation (UK GDPR / Data Protection Act 2018)
- UKCIS Guidance: *Sharing Nudes and Semi-Nudes: Advice for Education Settings Working with Children and Young People*

3. The Four Key Categories of Risk

In accordance with KCSIE 2026, online safety risks at Spring Bank Primary School are categorised into four core areas:

Risk Area	Description & Scope
Content *(Child as Recipient)*	Exposure to illegal, inappropriate, or harmful content, including: pornography, extreme physical/sexual violence, hate speech, misogyny, racism, antisemitism, self-harm, suicide encouragement, radicalisation, extremism, misinformation, disinformation

Risk Area	Description & Scope
	(fake news), and conspiracy theories.
Contact *(Child as Participant)*	Subjection to harmful online interaction from other users or Generative AI systems simulating human contact, including: peer pressure, commercial exploitation, online grooming, adult harassment, or adults posing as children/young adults to exploit pupils for sexual, criminal, or financial purposes.
Conduct *(Child as Actor)*	Personal online behaviour that increases the likelihood of, or causes, harm. This includes: online bullying, harassment, creating/uploading inappropriate material, sending or non-consensual sharing of explicit images (nudes/semi-nudes, including AI-generated imagery), illegal downloading, hacking, and financial scams.
Commerce *(Child as Consumer)*	Risks associated with commercial activity online, including: exposure to online gambling, inappropriate/aggressive advertising, illegal financial scams, phishing attacks, and harvesting of personal data.

4. Roles and Responsibilities

4.1 Governing Body

The Local Governing Board has overall responsibility for monitoring this policy and holding the Headteacher to account for its implementation. The Governing Body will ensure that:

- Online safety is an interrelated, continuous theme integrated into the school's whole-school approach to safeguarding.
- Appropriate filtering and monitoring systems are in place on all school network

infrastructure and devices, and that an annual review of their effectiveness is carried out by the Senior Leadership Team (SLT).
- Specific staff roles are assigned to manage and oversee filtering and monitoring systems.
- Teaching about online safety is appropriately adapted for vulnerable pupils and pupils with SEND.

4.2 Headteacher (Jordan License)

The Headteacher, Jordan License, is responsible for:

- Ensuring that all staff understand and implement this policy consistently across Spring Bank Primary School.
- Ensuring robust cover arrangements exist when the Designated Safeguarding Lead (DSL) is unavailable (e.g., dedicated, confidential shared safeguarding inbox).
- Assessing risk, sanctioning searches/confiscations of electronic devices where appropriate, and authorising any exceptions to standard IT/mobile phone rules.
- Overseeing complaints, disciplinary actions, and referrals to external agencies (such as the LADO or Police) where severe misuse or illegal material is identified.

4.3 Designated Safeguarding Lead (DSL) and Safeguarding Team

The DSL (Jordan License) and Deputy DSLs take operational responsibility for online safety and safeguarding by:

- Taking the lead on understanding and managing the filtering and monitoring systems and alerts generated across school devices.
- Ensuring all online safety incidents and safeguarding concerns are logged on CPoms and addressed promptly in accordance with the Child Protection Policy.
- Providing regular updates and annual safeguarding/online safety training to all staff.
- Liaising with external agencies, including Children's Social Care, the LADO, and Police, when required.

4.4 Technical / ICT Support Provider

Our contracted ICT Technical Support Provider (Datacable) is responsible for:

- Maintaining high-level technical security, including managed firewalls, antivirus software, and secure network infrastructure across both administrative and curriculum networks.
- Implementing filtering and monitoring mechanisms configured to block harmful and extremist content without unreasonably obstructing educational delivery.
- Carrying out routine system maintenance, security checks, and malware audits.
- Maintaining regular, secure, and off-site/cloud-based backups of all essential school data to ensure full recovery and operational continuity in the event of hardware failure, system corruption, or cyber incident.

4.5 All Teaching and Support Staff

All members of staff, contractors, and volunteers must:

- Maintain a current understanding of this policy and sign the Staff Acceptable Use Policy (AUP) annually.
- Maintain an attitude of 'it could happen here' regarding online abuse, cyberbullying, and harassment.
- Report any filtering failures, technical vulnerabilities, or online safety concerns immediately to the Headteacher (Jordan License) and DSL.
- Report any requirement to bypass filtering for legitimate educational research directly to the Headteacher prior to access.

4.6 Parents and Carers

Parents and carers are expected to support the school by reinforcing online safety expectations at home, endorsing the Pupil Acceptable Use Agreement, and raising any online safety worries or incidents with class teachers or the Headteacher.

5. Technical Infrastructure, Network Management, Filtering and Monitoring

---

5.1 Network Security and Access Control

- Spring Bank Primary School maintains two distinct network partitions: the Administrative Network and the Curriculum Network.
- Full access to administrative systems is restricted to the Headteacher (Jordan License) and authorised office staff via unique, strong credentials.
- All staff and pupils are assigned unique user credentials. Password sharing or logging in under another individual's identity is strictly prohibited.
- Multi-Factor Authentication (MFA)—such as entering a mobile authenticator code alongside their password—whenever accessing school email, Google Workspace, or cloud-based pupil management systems (such as CPOMS or Arbor) off-site or on personal devices.
- Guest users, visitors, and supply staff are granted restricted access subject to signing a Visitor AUP.

5.2 Filtering and Monitoring Provisions

- The school employs specialised filtering and monitoring software Datacable across all

school-owned devices and internet connections.

- System alerts for inappropriate keyword searches, denied domain attempts, or potential distress markers are automatically routed to the DSL and Headteacher.
- All staff and pupils are made aware that internet traffic and network activity on school devices are monitored and fully traceable to individual accounts.
- While Classroom Cloud provides automated device monitoring and generates real-time safety alerts, technical systems complement rather than replace direct adult oversight; teaching and support staff maintain primary responsibility for actively supervising pupil screen activity and online engagement during lessons
- When monitoring using Classroom Cloud, key staff will review all Urgent, High and Medium risk notifications. They may review Low risk, but this is not expected unless it is flagged by a child in a 'Vulnerable' group, which is decided by the senior leadership team.
- Urgent, High and Medium notifications must be categorised and may have a supporting comment. Notifications will be categorised as 'False Alarm' if there is no safeguarding concern raised, a comment may be added to explain context if key staff believe it is necessary. Notifications will be categorised as 'Completed' if there is clear intent to search inappropriate content or a concern needs further investigation.
- Urgent and High priority notifications will be sent to key staff via e-mail.

5.3 Artificial Intelligence (AI)

- In accordance with trust and school guidance, staff and pupils are expected to use AI tools responsibly and ethically.
- The primary approved AI platform for staff usage isGoogle Gemini.Chat GPT is also permitted providing no sensitive or personal information is used. Unsanctioned AI software or platforms are not permitted on school infrastructure.
- Misuse of AI tools—including the creation or dissemination of abusive content, 'deepfakes', or synthetic explicit imagery—will be treated as severe bullying/harassment and dealt with under the Behaviour Policy and Safeguarding procedures.

6. Managing Mobile Devices and Digital Technologies

6.1 Pupil Mobile Devices

Spring Bank Primary School operates a strict **mobile phone-free environment** by default:

- Pupils are strictly prohibited from using or accessing mobile phones, smartwatches, or devices with personal internet connectivity during the school day (including lessons, transitions, breaktimes, and lunchtimes).

- Any pupil bringing a mobile phone to school must surrender it upon arrival in accordance with school procedures, to be securely stored until home time.
- Any exceptions (e.g., essential medical tracking devices) must be formally submitted in writing and approved by the Headteacher, Jordan License.

6.2 Staff and Visitor Devices

- Staff members must not use personal mobile phones or personal digital cameras to record or capture photographs/videos of pupils.
- School-owned digital cameras or school devices must be used for all educational record-keeping and photography.
- Personal work devices taken off-site must remain password-protected, encrypted, and reserved exclusively for authorised professional use.

7. Cyberbullying

Cyberbullying is defined as the repetitive, intentional harm caused to an individual or group using digital communication platforms, social media, messaging apps, or gaming environments.

- Cyberbullying will be tackled proactively through the computing and PSHE curricula and addressed robustly under the school's Behaviour Policy.
- **Searching and Confiscation:** In accordance with DfE guidance and the Education Act 2011, the Headteacher (Jordan License) and authorised staff reserve the right to search electronic devices and delete inappropriate files/data where there is a 'good reason' to suspect the device poses a safety risk, undermines school discipline, or contains evidence of an offence.
- If a device is suspected of containing an indecent image of a child (nude or semi-nude), staff will **not view the image**, will confiscate the device immediately, and will report directly to the Headteacher/DSL for escalation to the police.

8. Educating Pupils: Online Safety Curriculum

Online safety education at Spring Bank Primary School is embedded across the curriculum, including Computing, PSHE, and dedicated assembly themes. Content is delivered in an age-appropriate manner, covering practical cybersecurity, privacy, digital literacy, and healthy online relationships.

Note: Specific timetable allocations and topic scheduling for discrete online safety modules across year groups are maintained in our separate Curriculum Long-Term Plan to reflect annual

context and pupil needs.

While pupils are strictly prohibited from directly operating generative AI platforms on school devices, the Key Stage 2 curriculum incorporates essential AI literacy within Computing and PSHE lessons. Pupils will be taught how artificial intelligence and synthetic media operate—including how manipulated images or videos ('deepfakes') are generated—and will develop critical thinking strategies to identify misleading information, bias, and digital content manipulation online.

Key Stage	Core Curriculum Focus Areas
Key Stage 1 (Years 1–2)	• Using technology safely, kindly, and respectfully. • Keeping personal information private and secure. • Recognising upset or unsafe content/contact and knowing how to report it immediately to a trusted adult.
Key Stage 2 (Years 3–6)	• Evaluating digital content critically (recognising fake news, misinformation, and online bias). • Understanding online relationships, social media age restrictions, and managing peer pressure. • Cybersecurity fundamentals: strong passwords, phishing awareness, and device security. • Recognising conduct risks, cyberbullying, and the permanent nature of digital footprints.

9. Handling Incidents and Misuse

- ---

  Minor Misuse: Minor breaches (e.g., unauthorised access to non-educational content, login misconduct) will be managed via standard disciplinary measures, parent notification, and temporary restriction of IT privileges.

- **Serious Misuse:** Major incidents (e.g., cyberbullying, accessing inappropriate/legal pornography, harassment) will result in formal disciplinary action, senior management involvement, logging on CPOMS, and potential permanent revocation of network access.
- **Illegal Activity & Indecent Images:** Discovery of illegal content (including indecent imagery of children, grooming attempts, or extremist radicalisation material) must be reported immediately to the Headteacher (Jordan License). The computer/device must be left untouched. The Headteacher will immediately inform the Police, LADO, and relevant local authority safeguarding partners. Staff must never conduct private investigations or forward suspect material via email.

In the event of a suspected cyber attack, malware infection, system intrusion, or unauthorised exposure of personal data:

- **Immediate Technical Reporting:** Any staff member noticing unusual network behaviour, ransomware messages, or system lockouts must notify the Headteacher (Jordan License) and DSL immediately, who will alert Data Cable without delay to isolate affected devices.
- **Data Protection Breach Notification (ICO):** If private or sensitive personal data relating to pupils, parents, or staff is compromised or exposed, the Headteacher will report the incident to the Information Commissioner's Office (ICO) within **72 hours** of discovery, in line with UK GDPR obligations.
- **National Cyber Reporting:** Severe cyber threats, illegal system intrusions, or extortion attempts will be reported to the **National Cyber Security Centre (NCSC)** and **Action Fraud**.

This Online Safety Policy was adopted by Spring Bank Primary School on 08/09/2026

Chair of Governors – Mr L Arnell		
Signature:		
Frequency of review:	Annual	
To be reviewed and approved by:	Spring Bank Primary School Local Governing Board	
Date of next review:	October 2027	

REVIEW RECORD

Date of review	Reason for review	Date of next review

Name:		**Signature:**	

On behalf of SBPS Full Board

Date of review	Reason for review	Date of next review

Name:		Signature:	

On behalf of SBPS Full Board

Date of review	Reason for review	Date of next review

Name:		Signature:	

On behalf of SBPS Full Board