

Leigh St. John's C.E. Primary School

Kirkhall Lane, Leigh, WN7 1RY

Headteacher: Mrs E. Lightfoot



ONLINE SAFETY, DIGITAL TECHNOLOGY AND ARTIFICIAL INTELLIGENCE POLICY

Safe • Responsible • Critical • Kind

Developed in consultation/advisory role with:	Governing Body, SLT, Staff, Pupils, Parents/Carers, LA and external services
For use by:	Pupils, Staff, Parents/Carers, Governors, Volunteers, Visitors and Service Providers
Reviewed:	Autumn Term 2026
Agreed by:	Full Governing Body – to be completed
Next policy review date:	Autumn Term 2027 (or sooner if guidance/technology changes)
Signed Chair of Governors:	<i>V Hilton</i>
Date:	19 October 2026

1. Introduction

This policy replaces the school's previous E-Safety Policy (reviewed September 2025). It reflects the significant changes in children's digital lives, statutory safeguarding expectations and national guidance since that review, including the rapid growth of generative artificial intelligence (AI), AI-generated content, smart technology and increasingly sophisticated cyber risks.

The term online safety is used throughout this policy. Online safety is an integral part of safeguarding and is not treated as a separate technical issue. This policy should be read alongside the school's Safeguarding and Child Protection Policy, Relationships and Behaviour Policy, Anti-Bullying Policy, Data Protection Policy, Computing Policy, Staff Code of Conduct, Mobile Phone arrangements and any acceptable-use agreements.

Core principle

Technology should enhance education without compromising safeguarding, privacy, professional judgement, equality, academic integrity or the quality of relationships between adults and children.

2. Aims and scope

The school aims to create a culture in which pupils and adults use digital technology safely, responsibly, critically and respectfully. The policy applies to school-owned and personal devices, school systems and accounts, online activity connected to school, and relevant conduct outside school where it affects a pupil, member of staff, the school community or the orderly running of the school.

- protect pupils and staff from online harm and support a strong safeguarding culture;
- ensure compliance with current data protection and information-security requirements;
- set clear expectations for the safe and responsible use of the internet, devices, online services, cloud systems, social media and AI;
- help pupils develop age-appropriate digital literacy, media literacy and AI literacy;
- ensure that filtering and monitoring are effective, proportionate and reviewed regularly;
- provide clear routes for reporting and responding to online-safety, safeguarding, data-protection and cyber-security incidents;
- ensure that staff understand that technology, including AI, supports but does not replace professional judgement and accountability.

3. The online risk landscape: the four areas of risk

In line with current safeguarding guidance, the school recognises four broad areas of online risk:

Area	Examples
Content	being exposed to illegal, inappropriate or harmful material, including pornography, violence, self-harm or suicide content, extremist material, misinformation and disinformation, hateful content, harmful challenges, AI-generated material and manipulated or synthetic media.
Contact	being subjected to harmful online interaction with other users, including peer pressure, bullying, grooming, exploitation, coercion, impersonation, scams and contact from adults or unknown users.
Conduct	personal online behaviour that increases the likelihood of, or causes, harm. This includes

	cyberbullying, sharing personal information, sexting/sharing nudes or semi-nudes, creating or sharing AI-generated or digitally altered sexual images, harassment, misuse of images, plagiarism and inappropriate use of AI.
Commerce	risks such as online gambling, inappropriate advertising, phishing, scams, financial exploitation, in-app purchasing and other commercial risks.

The school also recognises that online and offline safeguarding concerns frequently overlap. An incident that begins online may result in harm in school, at home or in the community, and vice versa.

4. Roles and responsibilities

4.1 Governing Body

- holds overall strategic responsibility for ensuring appropriate online-safety, filtering and monitoring arrangements are in place;
- ensures that filtering and monitoring provision is reviewed at least once every academic year and that the review involves the DSL, relevant SLT member, IT support and the responsible governor;
- receives appropriate assurance about online-safety incidents, filtering and monitoring, cyber-security, AI governance and staff training;
- ensures the school has regard to statutory guidance on mobile phones and other personal interactive communication devices.

4.2 Headteacher / Senior Leadership Team

- ensures this policy is implemented consistently and aligns with safeguarding, behaviour, data protection and curriculum expectations;
- identifies a senior leader with responsibility for digital technology governance and ensures appropriate oversight of AI use;
- ensures new technologies, including generative AI tools, are risk assessed before school adoption;
- ensures staff receive appropriate training on online safety, data protection, cyber security and AI;
- ensures serious online-safety, staff-conduct or safeguarding concerns are escalated through the appropriate procedures.

4.3 Designated Safeguarding Lead (DSL)

- has lead responsibility for safeguarding and child protection, including online safety;
- works with IT support and senior leaders to understand filtering and monitoring arrangements and how concerns are escalated;
- ensures that online child-on-child abuse, sexual harassment, sexual violence, sharing of nudes/semi-nudes and AI-generated sexual imagery are responded to as safeguarding concerns;
- contributes to the annual filtering and monitoring review and to risk assessment of pupil-facing AI.

4.4 Computing / Online Safety Lead and IT Support

- maintain the school's technical safeguards, devices, access controls and approved systems;
- work with the DSL and SLT to identify and manage digital risk;
- maintain and test filtering, monitoring, anti-malware, firewall, account security, backup and recovery arrangements;
- ensure that changes to filtering or monitoring are authorised, recorded and checked;
- support the review of AI products, cloud services and apps before they are introduced.

4.5 Staff

- use only approved systems and follow this policy and the Staff Code of Conduct;
- maintain professional boundaries in all digital communication;
- report online-safety, safeguarding, cyber-security and data concerns promptly;
- critically check AI-generated content before it is used or shared and remain professionally accountable for the final output;
- never enter personal, confidential or special-category data into an unapproved AI system.

5. Filtering and monitoring

The school will maintain appropriate filtering and monitoring systems on school-managed networks and devices. Filtering is preventative: it blocks access to illegal, inappropriate or potentially harmful content. Monitoring is reactive: it identifies activity or patterns that may indicate risk and enables timely safeguarding or technical action.

- Filtering and monitoring will reflect the age and needs of pupils, including SEND and EAL considerations, while avoiding unreasonable over-blocking that prevents effective teaching and safeguarding education.
- The school will review filtering and monitoring provision at least annually, and additionally whenever a safeguarding risk is identified, new technology or generative AI is introduced, working practices change, major software updates occur, or network/device configuration changes.
- The annual review will consider whether systems can manage dynamic, personalised and AI-generated content and will record findings and actions.
- Checks will be made from both safeguarding and technical perspectives and a record of checks will be retained.
- Staff may not disable, bypass or attempt to circumvent filtering or monitoring unless explicitly authorised for a legitimate professional purpose; any authorised exception must be recorded and reviewed.

At the date of this policy, the school's filtering and monitoring arrangements include systems provided through the school's IT support provider and Senso monitoring. The exact product names may change over time; any replacement must meet current DfE filtering and monitoring expectations and be subject to appropriate assurance before implementation.

6. Generative artificial intelligence (AI)

6.1 Principles

Generative AI can create text, images, audio, video, code and other digital content. It can support workload, planning and teaching, but it can also produce inaccurate, biased, unsafe, fabricated or copyrighted material. It can create highly convincing impersonations and manipulated media. Its use must therefore be deliberate, transparent where appropriate, and subject to human oversight.

- Safety, safeguarding and the best interests of children take priority over convenience or novelty.
- AI must not replace the professional judgement, subject knowledge or relational responsibilities of staff.
- Any school-adopted AI tool must have a clear educational or operational purpose and benefits that outweigh identified risks.
- Only school-approved AI tools may be used for school business where confidential, pupil-related or staff-related information could be involved.
- Age restrictions and terms of service must be followed. Primary-aged pupils must not be directed to create accounts for tools whose age requirements they do not meet.

6.2 Staff use of AI

Staff may use approved generative AI to support appropriate professional tasks, such as generating ideas, adapting non-sensitive resources, drafting generic communications or reducing routine administrative workload. The member of staff remains fully responsible for the accuracy, appropriateness, tone, copyright status and safeguarding implications of anything produced.

- AI outputs must be checked for factual accuracy, bias, discrimination, inappropriate content, safeguarding risk and suitability for the intended age group before use.
- No pupil name, date of birth, SEND information, safeguarding information, medical information, assessment record, family information, photograph, voice recording or other identifiable personal data may be entered into a general-purpose or unapproved AI tool.
- Identifiable images of pupils or staff must not be uploaded to AI image, video, voice-cloning or facial-generation tools unless the tool and purpose have been specifically approved following data-protection and safeguarding assessment.
- AI must not make final decisions about safeguarding, discipline, SEND provision, attendance action, admissions, staff performance or any other decision with significant effects on an individual. Human professional judgement and the relevant statutory process remain essential.
- AI must not be used to fabricate evidence, alter safeguarding records, create misleading communications purporting to come from another person, or conceal the source of professional work.
- Where AI materially contributes to a published or formal school document, staff should consider whether acknowledgement is appropriate and must ensure that no third-party intellectual property has been unlawfully reproduced.

6.3 Pupil use of AI

Evidence about the educational impact and safety of direct pupil use of generative AI continues to develop. At LSJP, pupil-facing use will therefore be cautious, purposeful and age appropriate.

- Pupils may use generative AI in school only when the activity has been planned and authorised by a member of staff and uses a school-approved, age-appropriate tool.
- Pupil use will be appropriately supervised. Staff will teach pupils that AI can be wrong, biased or misleading and that convincing content is not necessarily true.
- Pupils will be taught not to enter personal information, images, passwords or confidential information into AI systems.
- Pupils must not use AI to impersonate another person, create fake school messages, bully or harass others, generate sexualised or violent material, create deepfakes, or create/share nude or semi-nude images of real or fictional children.
- Pupils must not present AI-generated work as entirely their own where the teacher has not authorised such use. Expectations for independent work, homework and assessment will be made explicit by staff.
- Where AI is used to support learning, pupils will be taught to verify information using trusted sources and to explain how the tool contributed when asked.

6.4 AI safeguarding and product approval

- Before an AI product is introduced, leaders will consider its intended purpose, age appropriateness, safety features, content controls, filtering/monitoring compatibility, data handling, model-training arrangements, security, accessibility, bias, impact on cognitive/social development and terms of service.
- The school will refer to the DfE Generative AI Product Safety Standards when assessing AI products intended for educational use.
- Where an AI tool processes personal data, the school will consult the DPO and complete any required data-protection impact assessment (DPIA) before use.

- Unauthorised pupil use of AI on school systems will be managed through safeguarding, behaviour and curriculum procedures as appropriate rather than being treated solely as a technical breach.

7. Data protection, privacy and AI

The school will process personal data in accordance with UK data protection law, including the UK GDPR and Data Protection Act 2018 as amended by the Data (Use and Access) Act 2025. The school will follow current DfE data-protection guidance and advice from its Data Protection Officer.

- Personal data will be limited to what is necessary, held securely, kept accurate and retained only for as long as required.
- Staff will use approved school systems, including approved cloud storage, for school data. Personal email accounts and unapproved consumer cloud services must not be used for confidential school information.
- Personal data should not be entered into generative AI tools unless the use is strictly necessary, the tool is approved, the lawful basis and transparency requirements have been considered, and appropriate safeguards are in place.
- Where automated decision-making or profiling is contemplated, the school will be open and transparent and will seek advice from the DPO before implementation.
- Pupil and staff work, including text, images and other original creative material, must not be submitted for the purpose of training an AI model unless the school is satisfied that it has the necessary permission or a lawful exception applies.
- Data breaches must be reported immediately through the school's data-protection procedures so that the DPO can assess any reporting obligation to the ICO.

8. Cyber security

Cyber security is a safeguarding and operational-resilience responsibility as well as a technical responsibility. The school will work towards and maintain the DfE cyber-security core standards.

- complete a cyber-risk assessment annually and review it each term, and after significant incidents or changes;
- use secure account management and role-based access, removing or changing access promptly when staff leave or roles change;
- enable multi-factor authentication (MFA) for staff cloud-service accounts and IT administrative accounts in line with DfE standards;
- keep devices, operating systems and applications supported and updated, with anti-malware and firewall protection;
- provide regular cyber-security awareness training, including phishing, social engineering, password security and AI-enhanced scams;
- maintain a documented backup and recovery plan, including multiple copies and an off-site or appropriately separated backup, and test restoration arrangements termly;
- report cyber incidents promptly to senior leadership and IT support, and to external bodies where required.

9. Mobile phones, smart watches and personal devices

The school has regard to the statutory DfE guidance on mobile phones in schools. LSJP is a mobile phone-free environment for pupils throughout the school day. Pupils must not have access to or use mobile phones or other personal interactive communication devices during lessons, transition times, breaktimes or lunchtime, except where an agreed individual exception is required.

- Year 6 pupils who need a phone for independent travel may bring one only in accordance with school arrangements; it must be switched off and handed to staff for secure storage for the duration of the school day.
- Smart watches or other devices with messaging, calling, recording or similar interactive functionality are subject to the same expectations unless expressly permitted.
- Reasonable adjustments and exceptions will be made where necessary for disability, medical need or another justified individual circumstance.
- Staff personal phones must not be used to photograph or record pupils. Staff use during working time must remain professional and consistent with the Staff Code of Conduct.
- Parents/carers who need to contact a child during the school day should do so through the school office.

10. Digital images, video, audio and synthetic media

- School images and recordings of pupils will be captured, stored and published only in accordance with consent, safeguarding and data-protection arrangements.
- Staff should use school-owned or specifically authorised equipment for pupil images wherever possible. Personal-device use requires exceptional authorisation and prompt secure transfer/deletion.
- Pupils must not photograph, record or publish images/audio of others without permission.
- AI-generated or digitally altered images, videos and audio can be realistic. Pupils will be taught that images and recordings may be manipulated and should be evaluated critically.
- Creating or sharing deepfakes, sexualised synthetic media, voice clones or manipulated images of pupils or staff to humiliate, deceive, harass or sexualise another person is prohibited and may constitute a safeguarding concern or criminal matter.
- Any concern involving nude or semi-nude imagery, including AI-generated or digitally altered imagery, will be handled through safeguarding procedures.

11. Online communication, social media and professional boundaries

- Staff communication with pupils and families must use approved professional channels and accounts.
- Staff must not accept or initiate social-media connections with current pupils and must maintain appropriate boundaries with former pupils who remain children.
- Confidential or sensitive school matters must not be discussed on personal social media or messaging services.
- Official school social-media and website content must follow safeguarding, consent, copyright and data-protection requirements.
- Pupil names must not be combined with identifiable photographs in public posts unless there is a clear approved reason and appropriate consent and risk assessment.
- Online conduct outside school may be addressed where it affects the safety or wellbeing of pupils/staff, school relationships, the school's reputation or the orderly running of the school.

12. Teaching online safety and AI literacy

Online safety is taught through Computing, RSHE/PSHE and across the wider curriculum. Teaching is age appropriate and revisited as technology and pupils' experiences change.

- privacy, passwords, account security and personal information;
- how algorithms, search engines and recommendation systems can shape what users see;
- recognising misinformation, disinformation, scams, impersonation and AI-generated content;
- healthy technology habits and knowing when to seek help;
- copyright, ownership, plagiarism and respectful creation/sharing of digital content;

- cyberbullying, online child-on-child abuse, sexual harassment and safe reporting;
- age restrictions, safe use of apps and games, and online commercial risks;
- AI literacy: what generative AI is, why it can hallucinate or reflect bias, how to verify outputs, and why personal information should not be entered into public AI tools.

13. Staff training and awareness

- All staff will receive regular safeguarding and online-safety updates appropriate to their role.
- Staff with responsibility for filtering, monitoring, digital technology, data protection or safeguarding will receive role-specific training.
- AI training will cover safeguarding, data protection, intellectual property, bias, accuracy, cyber risks, professional accountability and approved-school-use expectations.
- Governors will receive sufficient information and training to provide appropriate strategic challenge and assurance.
- Parents/carers will receive regular information to support safe online behaviour at home, including emerging risks and the school's approach to mobile phones and AI.

14. Incident response and reporting

Any member of the school community who becomes aware of an online-safety concern should report it promptly. Staff must not investigate safeguarding concerns beyond what is necessary to establish immediate facts and preserve safety; the DSL will determine the appropriate safeguarding response.

- Immediate risk of harm: protect the child, inform the DSL without delay and contact emergency services where necessary.
- Child-on-child online abuse: record and refer to the DSL; consider support and risk management for all children involved.
- Nudes/semi-nudes or sexualised imagery: do not view, copy, print, forward or save imagery unnecessarily; follow safeguarding procedures and UKCIS guidance.
- AI-generated sexual imagery/deepfakes: treat as a safeguarding concern and consider police/other agency involvement where appropriate.
- Illegal online content: the DSL/Headteacher will consider referral to the police, CEOP and/or Internet Watch Foundation as appropriate.
- Staff conduct concern: follow KCSIE allegations/low-level-concerns procedures and contact the LADO where the threshold is met.
- Data breach or cyber incident: report immediately to senior leadership/IT and the DPO; preserve evidence and follow the school's incident-response and business-continuity arrangements.
- All incidents and actions will be recorded on the appropriate school system and reviewed for lessons, patterns and required policy/training changes.

15. Searching, confiscation and devices

Where a device is suspected of containing evidence of harmful, prohibited or illegal activity, staff will act in accordance with the school's Behaviour and Relationships Policy, current DfE searching/screening/confiscation guidance and safeguarding procedures. Staff will not routinely search through the content of a pupil's device without proper authority and consideration of safeguarding, privacy and evidential issues.

16. Procurement and approval of apps, cloud services and EdTech

- New apps, cloud services and AI products must be approved before use with pupils or school data.

- Approval will consider educational benefit, age suitability, safeguarding, filtering/monitoring compatibility, cyber security, accessibility, data protection, data-location/retention, advertising/commercial features, account requirements, supplier terms and exit arrangements.
- Products processing personal data will be considered with the DPO and appropriate contractual/data-processing arrangements put in place.
- Free consumer tools must not be assumed to be suitable for school use simply because they are widely available.

17. Monitoring, review and governance assurance

- This policy will be reviewed at least annually and sooner following significant statutory/guidance changes, serious incidents, major technology changes or introduction of significant new AI systems.
- The school will undertake and record an annual filtering and monitoring review involving SLT, DSL, IT support and the responsible governor.
- The school will periodically audit the AI tools being used by staff and pupils, including unofficial or emerging use, and update risk controls accordingly.
- The Governing Body will receive assurance that actions arising from reviews have been completed.

18. Key legislation and guidance

- Keeping Children Safe in Education 2026 (DfE) – statutory guidance.
- Generative artificial intelligence (AI) in education (DfE).
- Using AI in education: support for school and college leaders; Safe use of generative AI in education training materials (DfE, updated for 2026/27).
- Generative AI: product safety standards (DfE, updated January 2026).
- Meeting digital and technology standards in schools and colleges – filtering and monitoring, cyber security and digital leadership/governance standards (DfE, updated September 2026).
- Data protection in schools, including Generative AI and data protection in schools (DfE, updated July 2026).
- Mobile phones in schools (DfE statutory guidance, to be followed from September 2026).
- UK GDPR; Data Protection Act 2018 as amended by the Data (Use and Access) Act 2025.
- Online Safety Act 2023 and subsequent implementation where relevant to school online-safety education and reporting.
- Education for a Connected World (UKCIS), relevant UKCIS guidance on sharing nudes/semi-nudes, and current CEOP/IWF reporting routes.
- Computer Misuse Act 1990; Copyright, Designs and Patents Act 1988; Equality Act 2010; Prevent duty guidance.

Appendix 1 – Pupil Acceptable Use Agreement

These rules help us to use technology safely, kindly and responsibly. Staff will explain them in an age-appropriate way.

- I will use school devices and accounts only when I have permission and for the task I have been given.
- I will keep my password private and will not use another person's account.
- I will be kind and respectful when I communicate online.
- I will not share my full name, address, phone number, passwords, location or other private information online.
- I will not take or share photographs, video or audio of other people without permission.
- I will tell a trusted adult straight away if I see something that worries, upsets or confuses me, or if someone contacts me in a way that makes me uncomfortable.
- I understand that the school may filter and monitor activity on school systems and devices to help keep everyone safe.
- I will not try to bypass the school's security, filtering or monitoring systems.
- I will only use AI in school when a teacher has told me I may use an approved tool.
- I will never put personal information, photographs or passwords into an AI tool.
- I know AI can make mistakes and I will check important information with trusted sources.
- I will not use AI or any other technology to pretend to be someone else, bully someone, make fake messages or images, or create harmful/sexual content.
- I will be honest about my own work and will follow my teacher's instructions about when AI may or may not be used.
- I understand that if I deliberately break these rules, the school will respond in line with its safeguarding and behaviour policies.

Appendix 2 – Staff, Governors, Volunteers and Visitors: Acceptable Use

- I will use school systems and devices primarily for professional purposes and in accordance with school policies.
- I will protect passwords and use MFA where required. I will not share accounts or allow pupils to use staff credentials.
- I will use approved school systems for confidential information and will not move school data into personal email, unapproved cloud services or consumer apps.
- I will report phishing, suspicious messages, malware, cyber incidents, lost devices and data breaches immediately.
- I will use only approved AI tools for school business where any school information is involved.
- I will not enter identifiable pupil/staff data, safeguarding information, SEND/medical information, images or confidential material into an unapproved AI tool.
- I will critically review AI-generated output and remain professionally accountable for anything I use, publish or communicate.
- I will not use AI to fabricate evidence, automate significant decisions about individuals, create deceptive communications or generate inappropriate synthetic media.
- I will maintain professional boundaries online and will not use personal social-media or messaging accounts to communicate with pupils.
- I will not use personal devices to photograph or record pupils except where exceptional authorisation has been given and school procedures are followed.
- I understand that activity on school-owned systems/devices may be filtered, monitored, logged and reviewed for safeguarding, security and compliance purposes.
- I will comply with copyright, licensing, data-protection and intellectual-property requirements.

Appendix 3 – AI quick-check for staff

Before you use AI for school work, ask:

1. Is this an approved tool?
2. Am I about to enter personal or confidential data? If yes, stop unless the use has been specifically approved.
3. Does the task genuinely benefit from AI?
4. Could the output affect a child or adult significantly? If yes, human professional judgement must lead.
5. Have I checked accuracy, bias, safeguarding, copyright and age suitability?
6. Would I be comfortable explaining this use to a parent, governor, the DPO or an inspector?

Appendix 4 – Online Safety Incident Response

Step	Action
1. Make safe	If there is immediate danger, protect the child and contact emergency services if necessary.
2. Report	Inform the DSL for safeguarding concerns; IT/SLT for cyber incidents; DPO for data breaches; Headteacher/Chair as appropriate for staff concerns.

3. Preserve evidence	Do not unnecessarily view, copy or forward harmful imagery. Record factual information and preserve relevant technical evidence safely.
4. Assess and escalate	DSL/Headteacher decides on referrals to children's social care, police, LADO, CEOP, IWF or other agencies as appropriate.
5. Support	Provide proportionate support and safety planning for children and adults affected.
6. Record and review	Record decisions/actions, monitor for recurrence, and review whether filtering, training, curriculum or policy changes are needed.

Appendix 5 – Long-term loan of a school electronic device (staff)

A school-owned laptop, tablet or other device remains school property and is loaned for professional purposes. The member of staff agrees to:

- keep the device secure and in good condition and return it when requested or on leaving employment;
- use the device in accordance with this policy and the Staff Code of Conduct;
- keep the device password protected and use MFA where required;
- not install unapproved software, apps or hardware or reconfigure security settings;
- not allow family members or other unauthorised users to access school accounts or data;
- store school data only in approved locations and not on unencrypted removable storage;
- report loss, theft, damage, suspected compromise or unusual behaviour immediately;
- allow authorised school/IT staff to maintain, update, monitor or inspect the device where necessary;
- ensure school data is backed up through approved school arrangements rather than personal backup services.

Staff member name	
Username	
Device make/model	
Serial / asset number	
Staff signature and date	
Headteacher / authorised signature and date	

Filename: LSJP Online Safety AI Policy.docx
Directory: /Users/emmalightfoot/Library/Containers/com.microsoft.Word/Data/
Documents
Template: /Users/emmalightfoot/Library/Group
Containers/UBF8T346G9.Office/User Content.localized/Templates.localized/Normal.dotm
Title:
Subject:
Author: python-docx
Keywords:
Comments: generated by python-docx
Creation Date: 01/10/2026 16:20:00
Change Number: 2
Last Saved On: 01/10/2026 16:20:00
Last Saved By: E Lightfoot
Total Editing Time: 2 Minutes
Last Printed On: 01/10/2026 16:20:00
As of Last Complete Printing
Number of Pages: 12
Number of Words: 4,395
Number of Characters: 26,852 (approx.)