Online Safety and Acceptable Use Policy

Approved by Governors October 2026

To be reviewed annually
To be reviewed October 2027

Governor print _____

Governor signed_____ Date_____

1. Purpose and Scope

Online safety is an integral part of safeguarding and child protection at Joseph Turner Primary School. The school adopts a whole-school approach that protects and educates pupils, staff and the wider school community in their use of technology, and establishes clear arrangements to identify, report, intervene in and escalate concerns.

This policy applies to pupils, staff, governors, volunteers, visitors and contractors using school systems, networks, devices, accounts or online services, whether on or away from the school premises.

2. Effective Practice in Online Safety

- Education for the safe, responsible and appropriate use of technology by pupils and staff.
- An up-to-date and effectively implemented Online Safety and Acceptable Use Policy.
- Appropriate filtering and monitoring systems.
- Secure school networks, devices and user accounts.
- Appropriate safeguarding and online-safety training for staff.
- Age-appropriate online-safety education for pupils.
- Effective reporting and safeguarding procedures.
- Appropriate management of mobile and smart technology.
- Safe and appropriate use of generative artificial intelligence (AI).
- Regular review of emerging technologies and associated safeguarding risks.

3. Four Areas of Online Risk

Content

Exposure to illegal, inappropriate or harmful content, including pornography, racism, misogyny, self-harm, suicide, antisemitism, radicalisation, extremism, extreme sexual or physical violence, misinformation, disinformation and conspiracy theories.

Contact

Harmful online interaction with other users or generative AI applications that simulate interaction, including peer pressure, inappropriate commercial contact and grooming or exploitation for sexual, criminal, financial or other purposes.

Conduct

Online behaviour that increases the likelihood of, or causes, harm, including online bullying and the making, sending or receiving of explicit images, including material digitally altered or generated using AI.

Commerce

Risks including online gambling, inappropriate advertising, phishing, financial scams and other forms of online financial exploitation.

4. Leadership, Responsibilities and Review

Online safety forms part of the school's wider safeguarding arrangements and should be read alongside the Child Protection and Safeguarding Policy, Relational Policy, Anti-Bullying Policy, Staff Code of Conduct, Data Protection Policy, Computing Policy, mobile-device arrangements and relevant curriculum policies.

The Designated Safeguarding Lead (DSL, Lucy Cutler) has lead responsibility for safeguarding, including online safety. The DSL, Lucy Cutler works with the Headteacher, Laura Collins, Laura Collins, Computing Lead, Scott Sefton , Scott Sefton and IT support, Ian Grenhan Eservices, Ian Grenhan Eservices, to ensure appropriate arrangements are implemented.

The policy will be reviewed at least annually and sooner where there are significant changes in legislation, statutory guidance, technology, safeguarding risks or school systems.

5. Teaching and Learning

Technology is an important component of children's education and wider lives. Pupils will be supported to become safe, responsible, critical and digitally literate users of technology. Education will be appropriate to pupils' ages, developmental stages and individual needs, including the needs of pupils with SEND and other vulnerabilities.

Pupils will be taught to:

- understand acceptable and unacceptable online behaviour;
- protect personal information and privacy;
- recognise online bullying, harmful contact and inappropriate content;
- understand that people and information online may not always be what they appear to be;
- critically evaluate online information and cross-check accuracy;
- recognise misinformation, disinformation and potentially misleading AI-generated material;
- recognise phishing, scams, inappropriate advertising and other financial risks;
- understand opportunities and risks associated with generative AI;
- understand that images, audio and video may be altered or AI-generated;
- understand appropriate ways of creating, sharing and receiving images;
- know how and when to seek help and report concerns immediately to a trusted adult.

The Education for a Connected World framework may support curriculum planning alongside statutory RSHE and the wider curriculum.

6. Reporting Online Safety and Safeguarding Concerns

Pupils will be taught to tell a trusted adult immediately if something online makes them worried, uncomfortable, frightened or unsafe. Staff must take concerns seriously and follow the school's safeguarding procedures.

Any online concern indicating that a child may be suffering, or is likely to suffer, harm must be reported promptly to the DSL, Lucy Cutler or one of the deputy DSLs. Child-on-child online abuse will be considered as a safeguarding matter where appropriate and not solely as behaviour or ICT misuse.

Evidence should be preserved where safe and lawful to do so. Staff must not unnecessarily view, copy, forward or save potentially illegal or harmful imagery.

7. Generative Artificial Intelligence (AI)

The school recognises that generative AI can provide educational opportunities but may introduce safeguarding, privacy, information-security, accuracy and copyright risks.

- AI tools will be assessed before being approved for pupil use.
- The age, development and individual needs of pupils will be considered.
- Safeguarding and data-protection implications will be considered.
- Personal, sensitive or confidential information must not be entered into unapproved AI systems.
- Pupils will be taught that AI output can be inaccurate, misleading, biased or fabricated and should be checked against reliable sources.
- Inappropriate AI use will be addressed under safeguarding and/or behaviour procedures as appropriate.
- AI applications will be considered within filtering and monitoring arrangements.
- Staff will receive appropriate information, training and updates.

Creating, manipulating or sharing harmful or inappropriate AI-generated images, audio or video, including deepfakes, will be addressed under the school's safeguarding and behaviour procedures.

8. Filtering and Monitoring

The governing body will ensure that appropriate filtering and monitoring systems are in place and that relevant Department for Education filtering and monitoring standards are considered. The

filtering system will aim to block harmful and inappropriate content without unreasonably impacting teaching and learning.

- The Headteacher, Laura Collins in responsibile for filtering and monitoring
- The DSL, Lucy Cutler will have oversight of safeguarding implications.
- IT support, Ian Grenhan Eservices will provide appropriate technical expertise and support.
- Staff will understand how to report filtering and monitoring concerns.
- Arrangements will take account of school-owned devices and relevant internet-connected systems.
- The effectiveness of provision will be reviewed at least once every academic year by the responsible SLT member, supported by the DSL, Lucy Cutler and IT support, Ian Grenhan Eservices, and a record of the review and resulting actions will be retained.
- Weekly SENSO monitoring
- reports and IT reports produced three times a year will support operational oversight but do not replace the formal annual effectiveness review.

9. Mobile Phones, Smart Devices and Personal Technology

The school will maintain clear expectations concerning mobile phones, smart watches and other personal internet-connected devices. Devices using mobile data may bypass school filtering and monitoring systems. Pupils' use of personal devices will be managed through agreed school arrangements. Staff use of personal devices must comply with the Staff Code of Conduct and safeguarding procedures. Personal devices must not be used to photograph, film or record pupils unless explicitly authorised under an agreed school procedure.

10. Remote and Blended Learning

Where remote education is required, the school's safeguarding and child protection procedures continue to apply.

- Staff will use school-approved communication and learning platforms and school accounts.
- School devices will be used wherever practicable.
- Appropriate professional boundaries and privacy will be maintained.
- Personal contact information will not be shared with pupils.
- School procedures regarding recording lessons will be followed.
- Safeguarding concerns arising during remote learning will be reported through normal safeguarding procedures.
- Remote-learning technology will have appropriate privacy, security and safeguarding arrangements.

- Pupils will be reminded of the Acceptable Use Agreement and online-safety expectations.

11. Managing Internet Access and Information Security

- IT security will be supported by the school's approved IT support, Ian Grenhan Eservices provider.
- School ICT security will be reviewed regularly and security updates and malware protection maintained.
- Users must keep passwords secure and must not routinely share credentials. Authorised administrators may reset or manage accounts when necessary.
- Pupils must immediately tell a trusted adult if they receive offensive or inappropriate electronic communication and must not deliberately delete relevant evidence.
- Pupils will be taught not to disclose personal details about themselves or others and not to meet an online contact without appropriate adult knowledge and safeguards.
- Suspicious messages, links and attachments should be treated cautiously.

12. Images, Recordings and Published Content

Photographs, video and audio recordings of pupils will only be created using school-approved devices, systems and accounts unless alternative arrangements are specifically authorised by the Headteacher, Laura Collins.

- Images and recordings must have a legitimate educational or school purpose.
- They must be stored securely and only be accessible to authorised persons.
- They will be managed in accordance with the Data Protection and Records Management policies.
- They must not be stored permanently on personal devices.
- They will be securely deleted when no longer required in accordance with retention arrangements.
- Publication will take account of current consent arrangements, safeguarding considerations and data-protection requirements.
- Staff or pupil personal contact information will not be published. The school's official contact details should be used online.

13. Social Networking and Personal Publishing

- Pupils, staff and parents/carers will receive age-appropriate information about safe use of social networks and online services.
- Staff must maintain professional boundaries and must not use personal social-media relationships to communicate with pupils.

- Pupils will be taught not to disclose information that identifies themselves, friends or their location.
- Parents/carers will be signposted to current provider age requirements and safety information rather than relying on a fixed list that may become outdated.
- Significant emerging online-safety information will be shared with families when appropriate.

14. Protecting Personal Data

Personal data will be collected, processed, stored, shared and disposed of securely and lawfully in accordance with UK GDPR, the Data Protection Act 2018, the school's Data Protection Policy and relevant Department for Education guidance.

15. Authorising Internet and System Access

- Staff must read and sign the Staff Acceptable Use Agreement.
- Parents/carers and pupils will be provided with the relevant home-school online-safety or acceptable-use agreement.
- Pupil access will be appropriately supervised and supported according to age, developmental stage and need.
- Visitors or others requiring access to school systems will be expected to comply with the school's acceptable-use and security arrangements.

16. Risk Assessment and Incident Management

The school will take reasonable precautions to prevent access to harmful or inappropriate material while recognising that no technical system provides absolute protection. Online-safety incidents will be assessed according to their nature and level of risk.

- Safeguarding concerns must be reported immediately to the DSL, Lucy Cutler or one of the deputy DSLs.
- Where there is an immediate risk of harm, appropriate emergency safeguarding action will be taken.
- Where potential criminal activity is identified, the Headteacher, Laura Collins/DSL, Lucy Cutler will consider referral to the police and/or relevant agencies in accordance with safeguarding procedures.
- Staff must not intentionally view, download, copy, forward or share illegal or suspected illegal imagery in an attempt to investigate an incident.
- Parents/carers and pupils will be informed of relevant reporting and complaints procedures.

17. Staff Training and Communication

All staff will receive appropriate safeguarding and online-safety information through induction and regular safeguarding updates and training. All staff must read Part One of Keeping Children Safe in Education 2026 in full.

- Training will address the four areas of online risk;
- filtering and monitoring responsibilities;
- reporting of online-safety concerns;
- child-on-child online abuse;
- generative AI and AI-generated/manipulated imagery;
- professional boundaries;
- data protection and cyber security;
- emerging online risks; and
- the particular vulnerabilities of individual pupils.

18. Working with Parents and Carers

The school will work in partnership with parents and carers, provide relevant online-safety information throughout the year and signpost families to current sources of support. Parents/carers are encouraged to establish age-appropriate boundaries around devices, gaming, messaging, social media and emerging technologies and to contact the school where they have concerns.