Leigh St Peter's CE Primary School
Online Safety Policy

Member of Staff Responsible:	Senior Leadership Team
Signed (Chair of Governors'):	Julie Williams
Signed (Headteacher):	Kevin Robinson
Date Policy Adopted:	September 2025
Policy Review Date:	July 2026

Vision & Values:

Our Christian Vision is to provide a happy, safe, and caring high quality learning environment where all members of the school community have the opportunity to flourish; 'living life in all its fullness'. Our Christian Values have been developed in line with everyone who is invested in our school community: its pupils, parents', staff, and governors and we aim to ensure that these Christian Values are at the heart of everything we do at Leigh St Peter's CE Primary School.

Outline:

At Leigh St Peter's CE Primary School, safeguarding pupils is at the core of our vision. Online safety is not treated as a standalone issue but as part of the school's overarching safeguarding responsibilities. This policy ensures that pupils and staff use technology responsibly, safely, and effectively in line with:

- NSPCC guidelines for online safety
- National Crime Agency's CEOP Education programme
- KCSIE 2025 and the School Safeguarding and Early Help Policy
- PolEd (Police Education Programme)
- UKCIS "Education for a Connected World"
- Data Protection Act 2018 & UK GDPR

Aims:
- Protect pupils from online harm.
- Promote responsible use of digital technologies.
- Equip staff with the training and resources to safeguard pupils.
- Educate pupils and parents on safe online practices.
- Ensure school devices and systems are used securely and appropriately.

Roles and Responsibilities

Governing Board	Headteacher	All Staff	Computing Lead	Pupils	Parents/Carers
Reviews and approves the online safety policy.	Oversees online safety implementation and response. Ensures integration into wider safeguarding practice. Manages monitoring and filtering systems.	Maintain vigilance and report concerns.	Manages the e-safety awareness curriculum in school	Follow Acceptable Use Agreements and report concerns.	Support safe use at home and engage with school guidance.

Teaching Online Safety

Online safety is taught through the PSHE and Computing curriculum using:
- *CEOP's "ThinkUKnow"*
- *NSPCC's "Share Aware" and "Speak Out Stay Safe"*
- *PolEd sessions (Police Education Programme)*
- *UKCIS "Education for a Connected World" framework*

Topics include:
- *Healthy online relationships*
- *Digital footprint and reputation*
- *Managing harmful content*
- *Reporting unsafe behaviour online*

Filtering and Monitoring
To maintain a safe digital environment, we use Senso.cloud for monitoring and filtering.

Senso.cloud:
- Filters harmful/inappropriate content.
- Monitors staff and pupil activity in real time.
- Sends real-time alerts to safeguarding leads.
- Offers custom filters per age group and reporting tools.

Staff Responsibilities:
- Must not bypass filtering/monitoring.
- Must respond to alerts per safeguarding procedures.

Device Coverage:
- All school-issued devices are monitored on and off premises.

Review:
- Monitoring data is reviewed regularly by DSL and Computing Lead in school.

Acceptable Use:
All users sign Acceptable Use Agreements outlining appropriate and safe behaviour online.
- Pupils, staff, visitors are covered.
- Misuse may result in disciplinary or safeguarding procedures.
- Remote learning tools and communication must be school approved.

Use of School-Issued Electronic Devices:
To maintain high standards of data security and safeguarding:
- Devices must only be used by the assigned staff member.
- Not to be accessed by other staff or household members.
- Not to be used for non-work-related purposes.
- Staff must keep devices secure and report breaches immediately.
- Devices must be returned during long-term absences (over 2 weeks).

Staff Online Safety:
- Staff model safe online behaviour.
- Personal-professional boundaries must be respected.
- Staff must use school platforms for communication.
- Training includes grooming, sexting, phishing, cyberbullying.
- Concerns are reported to DSL and investigated.

Managing Incidents
- All online safety incidents must be reported to the DSL. This includes cyberbullying, grooming, sexting, exposure to harmful content.
- Responses follow safeguarding and behaviour policies. Referral to external agencies where appropriate (e.g. CEOP, social care).

Remote Learning & Use of Devices
- School-approved platforms used (e.g. Seesaw, TT Rockstars, etc).
- Safeguards include supervised access and recording of live sessions. Devices must adhere to filtering/monitoring protocols.

Parental Engagement
- Parents receive training, updates and resources through the school's weekly newsletter.
- School promotes NSPCC, Internet Matters and UK Safer Internet Centre.
- Parental involvement is crucial to reinforcing safe online behaviour.

Policy Review and Evaluation
- Reviewed annually by DSL and Governing Board. The policy is informed by new legislation, national guidance, incident trends and stakeholder feedback.

Linked Policies
- Child Protection and Safeguarding Policy
- Staff Code of Conduct
- Behaviour and Anti-Bullying Policy
- Acceptable Use Policies (Staff, Pupils, Visitors)
- Data Protection Policy
- Remote Learning Policy
- Mobile Phone Policy