



EDUCATION
EAST SUSSEX
TOGETHER FOR EXCELLENCE
AND INCLUSION



Online Safety Roles and Responsibilities Schedule

Alfriston Primary School

This policy was adopted on 30th September 2026

This policy is due for review on 1st September 2027



Purpose of this schedule

This schedule sets out who is responsible for the strategic oversight, implementation, safeguarding response, technical delivery, education and assurance of online safety. It should be read alongside the Core Online Safety Policy and the linked standards and procedures. It is intentionally role-based so that settings can adapt titles without changing the underlying allocation of responsibility.

Online safety is a shared responsibility. No single role - including the DSL or IT provider - can discharge the setting's responsibilities alone. Governance, safeguarding, technical controls, curriculum, staff conduct, data protection and family engagement must work together.

Where responsibilities are outsourced, the setting remains accountable for ensuring that the relevant functions are delivered, evidenced and reviewed.

1. Responsibility principles

Principle	What this means
Strategic accountability	The governing board holds strategic responsibility for safeguarding and seeks assurance that online safety arrangements are effective.
Safeguarding leadership	The DSL holds lead safeguarding responsibility for online safety and for the safeguarding response to concerns, alerts and incidents.
Digital and technical governance	A named senior leader oversees digital strategy and the strategic management of filtering and monitoring. Technical staff or provider's advice, implement, maintain, test and report; they do not replace leadership or safeguarding judgement.
Data protection	The DPO advises on lawful processing, privacy, DPIAs, information sharing, records and personal data breaches.
Education and supervision	Curriculum leaders and all staff ensure that online safety education, supervision and professional practice support the setting's safeguarding objectives.
Shared responsibility	Children, parents, carers, visitors, volunteers and contractors are given clear expectations appropriate to their role and access.

2. Roles and responsibilities

The table below provides the default allocation of responsibilities.

Role	Core responsibilities	Assurance / reporting	Key linked documents
Governing board	Holds overall strategic responsibility for safeguarding and online safety; ensures appropriate policies, procedures and resources are in place; assigns appropriate leadership and governor oversight; ensures the setting meets applicable statutory safeguarding and digital-technology expectations.	Receives assurance on online safety, filtering and monitoring, cyber risk, significant incidents, staff training and improvement actions; considers the outcome of the annual filtering and monitoring review; challenges unresolved risks and confirms actions are followed through.	Core Online Safety Policy; Filtering and Monitoring Standard; Cyber Security Standard; annual assurance records.
Named governor for safeguarding or online safety	Provides focused oversight on behalf of the governing board; develops sufficient understanding of online safety, filtering and monitoring and emerging technology risks to provide effective challenge.	Meets or receives updates from relevant leaders and the DSL; reviews evidence rather than relying solely on verbal assurance; reports key issues back to the governing board.	Roles Schedule; Filtering and Monitoring Annual Assurance Checklist; safeguarding reports.
Headteacher	Provides accountable leadership for implementation of the policy suite; promotes a culture in which online safety is part of safeguarding; ensures	Receives reports on significant concerns and risks; ensures actions from reviews, audits and incidents are completed; escalates strategic	Core Online Safety Policy; risk register; safeguarding and digital strategy documents.

Online Safety Roles and Responsibilities Schedule

Role	Core responsibilities	Assurance / reporting	Key linked documents
	responsibilities are assigned, understood and resourced; ensures online safety is considered in behaviour, curriculum, staffing, procurement, risk management and business continuity.	risks to governors as appropriate.	
Senior leader responsible for digital strategy / IT	Owns day-to-day strategic governance of digital technology and cyber security; coordinates risk, procurement and assurance; ensures technical services support safeguarding, accessibility, continuity and data protection; works with the DSL, DPO and IT provider.	Maintains or coordinates digital/cyber risk information; reports significant risks and improvement actions to leadership and governance; seeks evidence from IT providers and suppliers.	Cyber Security and Account Management Standard; procurement/change processes; risk register.
Named SLT lead for filtering and monitoring	Leads the strategic management of filtering and monitoring; oversees procurement decisions and the rationale for what is blocked or allowed; ensures roles, reporting routes and staff awareness are clear; leads the formal review with support from the DSL and IT.	Ensures the effectiveness of filtering and monitoring is formally reviewed at least once every academic year; records outcomes and actions; ensures high-risk alerts and routine reports have documented routes; reports assurance to governors/proprietor .	Filtering and Monitoring Standard and Annual Assurance Checklist.

Online Safety Roles and Responsibilities Schedule

Role	Core responsibilities	Assurance / reporting	Key linked documents
Designated Safeguarding Lead (DSL)	Holds lead safeguarding responsibility for online safety; understands the setting's online risk profile and filtering/monitoring arrangements; leads the safeguarding response to online concerns; ensures online and offline indicators are considered together; coordinates referrals and information sharing where required.	Reviews or ensures appropriate triage of safeguarding alerts and concerns; records decisions and actions; identifies patterns and curriculum/training implications; contributes to the annual filtering and monitoring review; reports safeguarding themes and risks to leaders and governors.	Core Online Safety Policy; Incident Response Procedure; Local Safeguarding Contacts and Referral Schedule; Filtering and Monitoring Standard.
Deputy DSL	Supports the DSL and acts in accordance with delegated safeguarding responsibilities; ensures effective safeguarding cover when the DSL is unavailable; responds to online safety concerns within the setting's safeguarding arrangements.	Records and escalates concerns consistently; contributes to pattern identification and review as requested by the DSL.	Incident Response Procedure; safeguarding recording arrangements.
Data Protection Officer	Advises on UK GDPR and Data Protection Act requirements, privacy, lawful processing, information sharing,	Receives or advises on suspected personal data breaches; contributes to DPIAs and procurement	Data Protection Policy; privacy notices; retention schedule; DPIAs; Cyber Security Standard; AI

Online Safety Roles and Responsibilities Schedule

Role	Core responsibilities	Assurance / reporting	Key linked documents
	DPIAs, data breaches, retention and third-party processing; supports assessment of new technology, AI, monitoring and communications tools.	reviews; reports significant privacy risks and required actions through the setting's governance arrangements.	Procedure.
Managed Service Provider	Provides technical expertise; configures, maintains and tests agreed controls; supports secure accounts, devices, networks, filtering, monitoring, backups and incident response; provides clear advice on capability, limitations and unresolved technical risks; implements decisions authorised by the setting.	Provides evidence, logs, reports and incident information to the appropriate setting leads; escalates significant technical risks promptly; supports annual reviews and assurance; documents agreed technical changes.	Filtering and Monitoring Standard; Cyber Security and Account Management Standard; service contract / SLA; cyber incident response arrangements.
Curriculum / Computing / PSHE / RSE leads	Ensure online safety is taught through a planned, progressive and age-appropriate curriculum; identify opportunities across subjects; ensure teaching reflects current risks, digital literacy, AI, healthy relationships and reporting routes.	Reviews curriculum coverage and progression; uses pupil voice, safeguarding themes and emerging risks to identify gaps; reports curriculum actions to senior leaders.	Core Online Safety Policy; curriculum maps; Teaching Online Safety guidance; Education for a Connected World.
SENCO	Advises on additional online vulnerabilities, accessibility, assistive	Contributes to individual risk assessments or plans	Core Online Safety Policy; SEND/inclusion

Online Safety Roles and Responsibilities Schedule

Role	Core responsibilities	Assurance / reporting	Key linked documents
	technology and reasonable adjustments; supports staff to adapt education, supervision and controls to individual needs without unnecessarily restricting access.	where needed; advises DSL, curriculum staff and technical leads where safeguards or controls require adjustment.	procedures; individual plans and risk assessments.
All staff	Treat online safety as part of safeguarding; follow the policy and acceptable-use expectations; use authorised accounts, systems and communication routes; maintain professional boundaries; supervise technology appropriately; protect data and devices; report concerns promptly and do not assume technical controls will identify every risk.	Complete required training and updates; report safeguarding, cyber and data concerns through the correct route; cooperate with reviews and incident response; identify where policy or controls create practical difficulties.	Staff Online Safety Quick Guide; Staff Acceptable Use Agreement; Incident Response Procedure; Cyber Security Standard; Communications Procedure; AI Procedure.
Staff with monitoring / alert-triage responsibilities	Review monitoring information in accordance with documented thresholds and routes; apply safeguarding judgement; distinguish routine technical information from safeguarding concerns; ensure high-risk	Keep proportionate records of action; escalate technical limitations or repeated patterns; contribute evidence to review and assurance.	Filtering and Monitoring Standard; Incident Response Procedure.

Online Safety Roles and Responsibilities Schedule

Role	Core responsibilities	Assurance / reporting	Key linked documents
	concerns reach the DSL/DDSL promptly.		
Children	Use technology, accounts and devices responsibly; follow age-appropriate acceptable-use expectations; respect others; protect their login information; follow rules on AI and personal devices; tell a trusted adult when something online worries them or when they make a mistake.	Take part in online safety education and pupil voice opportunities; report concerns, harmful content, suspicious activity or account problems to staff.	Age-appropriate Pupil Acceptable Use Agreement; curriculum materials.
Parents and carers	Support children to use technology safely and responsibly; reinforce age-appropriate boundaries; engage with setting communications and agreements; raise concerns with the setting and provide relevant information where an online issue affects their child.	Use the setting's agreed communication and reporting routes; work with the setting during safeguarding responses where it is appropriate and safe to do so.	Parent/Carer Agreement; Core Online Safety Policy; Local Safeguarding Contacts and Referral Schedule.
Visitors and volunteers	Follow the setting's local rules for devices, photography, recording, network access, communications and confidentiality; use technology only as	Comply with induction or sign-in information and the Visitor/Volunteer Acceptable Use Agreement; report concerns to the named setting	Visitor/Volunteer Agreement; Mobile Phone and Personal Device Policy.

Online Safety Roles and Responsibilities Schedule

Role	Core responsibilities	Assurance / reporting	Key linked documents
	authorised; report safeguarding concerns immediately.	contact or DSL.	
Contractors and third-party education / community providers	Comply with contractual and local safeguarding, online safety, data protection and technology requirements; ensure staff understand professional communication expectations; protect any access to setting systems or information.	Provide assurance or evidence where required; report incidents, breaches or safeguarding concerns promptly; cooperate with investigations and review.	Contracts / service agreements; Community-use arrangements; Cyber Security Standard; Data Protection documents.
Local authority	Provides strategic oversight, guidance, commissioning or shared services where these functions sit above the setting; may provide broadband, filtering, safeguarding, DPO, IT or assurance support depending on local arrangements.	Defines service responsibilities clearly; provides appropriate evidence and escalation routes; supports settings to understand what remains locally accountable.	Local service arrangements; SLAs; Local Safeguarding Contacts and Referral Schedule.

3. Who leads when an issue occurs?

Some incidents involve more than one route. The table below identifies the primary lead, but roles should work together where safeguarding, cyber security, data protection, behaviour or staff conduct overlap.

Issue	Primary lead	Support / consultation	Key principle
Safeguarding concern about a child arising online	DSL / DDSL	Relevant pastoral staff; IT where technical evidence or controls are involved	Follow the Incident Response Procedure and local safeguarding referral routes.
Filtering or monitoring alert with potential safeguarding significance	DSL / DDSL	Named SLT filtering/monitoring lead; IT	Technical staff provide context; safeguarding staff decide the child-centred response.
Filtering configuration / blocked or allowed content decision	Named SLT filtering/monitoring lead	DSL; curriculum lead; IT	IT advises and implements. Strategic decisions remain with the setting.
Cyber security incident	Senior leader responsible for digital / cyber incident lead	IT/MSP; DPO; DSL where safeguarding implications arise	Cyber and safeguarding routes may operate in parallel.
Personal data breach	DPO / Data Protection Lead with accountable senior leader	IT; DSL where safeguarding implications arise	Follow the setting's personal-data-breach procedure.
Concern about staff online conduct or professional boundaries	Headteacher / appropriate senior leader	DSL; LADO or equivalent where thresholds are met; HR as appropriate	Follow staff allegations / low-level concerns / code of conduct arrangements.
AI-related safeguarding concern	DSL / DDSL	AI/digital lead; IT; DPO depending on the issue	Treat the harm according to its nature, not simply because AI was used.

Issue	Primary lead	Support / consultation	Key principle
AI tool approval / procurement	Senior leader / digital lead	DSL; DPO; IT; curriculum lead	Assess purpose, age restrictions, safeguarding, privacy, security, accessibility and educational benefit.
Mobile phone or personal-device behaviour issue	Relevant behaviour / pastoral lead	DSL where there is a safeguarding concern	Follow the Mobile Phone and Personal Device Policy; lawful search/confiscation powers vary by setting type.
Illegal or suspected illegal online content	DSL / DDSL	Police or other statutory body as required; IT to preserve systems/evidence where instructed	Staff should not conduct their own investigation or unnecessarily view illegal material.

4. Minimum assurance cycle

This table is a practical summary of the recurring assurance activity expected across the online safety framework. Settings may combine these activities within existing safeguarding, risk or governance cycles.

Frequency / trigger	Assurance activity	Lead	Oversight
At least annually	Review the Core Online Safety Policy and linked procedures; consider statutory changes, incidents, emerging risks, accessibility and stakeholder feedback.	Policy owner / DSL / senior leadership	Governing board / proprietor
At least once every academic year	Formal review of filtering and	Named SLT filtering/monitoring	Governing board / responsible governor

Online Safety Roles and Responsibilities Schedule

Frequency / trigger	Assurance activity	Lead	Oversight
	monitoring effectiveness, including devices, users, locations, off-site use and relevant AI activity.	lead with DSL and IT	
At least annually	Cyber risk assessment and assurance review; confirm significant risks, controls, recovery arrangements and improvement actions.	Senior digital/cyber lead with IT/MSP	Senior leadership and governors
Regular / termly as appropriate	Review significant online safety incidents, patterns, vulnerabilities, training needs and curriculum implications.	DSL / DDSL	Senior leadership / safeguarding governor
On induction and through regular updates	Online safety, safeguarding, filtering/monitoring awareness, cyber security and professional-use expectations.	DSL / relevant training leads	Senior leadership
Before introducing significant new technology or AI	Assess safeguarding, privacy, security, accessibility, age restrictions, educational purpose and filtering/monitoring implications.	Authorised senior leader	DSL, DPO and IT as appropriate
After a significant incident or material	Review relevant controls, risk	Relevant lead depending on	Senior leadership / governing board

Frequency / trigger	Assurance activity	Lead	Oversight
change	assessments, procedures, training and lessons learned.	incident	where significant

5. Local role allocation

Responsibility	Local allocation
Headteacher	Lindsey Hudson
DSL	Lindsey Hudson
Deputy DSL	Tanya Fitzgerald
Named SLT lead for filtering and monitoring	Tanya Fitzgerald
Named governor responsible for filtering and monitoring	Jeanette Adams
Senior leader responsible for digital strategy / cyber security	Lindsey Hudson/Tanya Fitzgerald
Service desk	Schools ICT, ESCC
DPO	Roger Simmons
Curriculum lead(s) for online safety	Lindsey Hudson
SENCO	Caroline Caley
Local safeguarding / LADO / Prevent / police contacts	See Incident Response Procedure, Appendix D. Local contacts and escalation.