



Meadow View Farm School
excellence as standard

Online Safety Policy

& Acceptable Use Agreements

2026/27

School	Meadow View Farm School
Adopted	May 2017
Current review	September 2026
Next review	September 2027, or earlier if guidance changes
Policy owner	Headteacher / Designated Safeguarding Lead
Approved by	Proprietary Body

This policy should be read alongside the Child Protection and Safeguarding Policy, Behaviour & Regulation Policy, Anti-Bullying/Incidents of Hate Policy, Staff Code of Conduct, Data Protection Policy and relevant curriculum policies.

Contents

1. Aims and scope
2. Statutory framework and related guidance
3. Online safety risks: the 4Cs
4. Roles and responsibilities
5. Filtering and monitoring
6. Artificial intelligence and emerging technology
7. Online safety curriculum
8. Supporting pupils with SEND, SEMH and additional vulnerabilities
9. Child-on-child online abuse and cyberbullying
10. Reporting and responding to concerns
11. Searching devices and harmful or illegal content
12. Mobile phones and personal devices
13. Staff use of technology and work devices
14. Working with parents and carers
15. Data protection, privacy and cyber security
16. Training
17. Monitoring, review and annual risk assessment
18. Links with other policies
- Appendix 1: Stage 1 pupil acceptable use agreement
- Appendix 2: Stage 2 & 3 pupil acceptable use agreement
- Appendix 3: Staff, Proprietary Body, volunteers and visitors acceptable use agreement
- Appendix 4: Online safety training needs self-audit
- Appendix 5: Online safety incident record

1. Aims and scope

Meadow View Farm School (MVFS) is committed to safeguarding and promoting the welfare of children online as well as offline. Technology is an important part of learning, communication and daily life. Our approach is to enable pupils to benefit from technology while reducing the risk of harm through education, appropriate supervision, technical controls and clear safeguarding procedures.

- protect and educate pupils, staff, volunteers and the wider school community in the safe, responsible and positive use of technology;
- ensure online safety is embedded within the school's whole-school safeguarding approach;
- identify, report, respond to and escalate online safety concerns appropriately;
- maintain appropriate filtering and monitoring arrangements without unreasonably restricting teaching and learning;
- teach pupils the knowledge, behaviours and help-seeking skills they need to become increasingly safe and resilient online; and
- provide a personalised and developmentally appropriate approach for pupils with SEND, SEMH and other vulnerabilities.

Scope: This policy applies to school-owned devices, school networks and systems, online activity undertaken as part of school provision, and relevant online behaviour outside school where it creates a safeguarding, welfare, conduct or school-community concern.

2. Statutory framework and related guidance

This policy has been reviewed for the 2026/27 academic year with regard to current statutory and Department for Education guidance, including:

- Keeping Children Safe in Education 2026 (in force from 1 September 2026);
- Relationships Education, Relationships and Sex Education (RSE) and Health Education statutory guidance (revised guidance in force from 1 September 2026);
- DfE Filtering and Monitoring: Core Standard (updated 25 August 2026);
- DfE Generative AI: Product Safety Standards;
- Teaching online safety in schools;
- Searching, screening and confiscation: advice for schools;
- UKCIS guidance on sharing nudes and semi-nudes;
- Prevent duty guidance and guidance on protecting children from radicalisation;
- Education Act 1996, Education and Inspections Act 2006, Education Act 2011, Equality Act 2010, Data Protection Act 2018 and UK GDPR, as applicable.

The school will apply the most recent version of statutory guidance where it supersedes wording in this policy.

3. Online safety risks: the 4Cs

MVFS uses the 4Cs framework to understand online risk. Risks may overlap and may occur on school systems or outside school.

Content

Exposure to illegal, inappropriate or harmful material, including pornography, violent or hateful content, racism, misogyny or misandry, antisemitism, self-harm or suicide content, extremism, misinformation, disinformation, conspiracy theories, deepfakes and AI-generated material.

Contact

Harmful interaction with other users, including peer pressure, grooming, exploitation, sextortion, scams, adults posing as children, and sexual, criminal or financial exploitation.

Conduct

Online behaviour that causes or increases harm, including bullying, harassment, discriminatory abuse, unsafe image sharing, sexual harassment, coercive behaviour, impersonation and creation or distribution of harmful or sexualised AI-generated content.

Commerce

Commercial and financial risks including gambling, loot boxes, inappropriate advertising, phishing, scams, fraud, in-app purchasing and manipulative or persuasive design.

4. Roles and responsibilities

4.1 Proprietary Body

The Proprietary Body has overall responsibility for ensuring that safeguarding arrangements, including online safety, are effective and that the Headteacher is held to account for implementation. It will:

- ensure online safety is a running and interrelated theme within safeguarding;
- ensure appropriate filtering and monitoring systems are in place and review the DfE filtering and monitoring standards;
- ensure roles and responsibilities for filtering and monitoring are identified and understood;
- receive appropriate safeguarding training, including filtering and monitoring;
- ensure provision is adapted where a one-size-fits-all approach is unsuitable, particularly for vulnerable pupils and pupils with SEND;
- receive assurance that the annual filtering and monitoring review and online safety risk assessment have been completed and actions followed up.

4.2 Headteacher

The Headteacher is responsible for ensuring this policy is understood and implemented consistently, that appropriate resources and training are available, and that serious concerns are escalated appropriately.

4.3 Designated Safeguarding Lead (DSL)

The DSL takes lead responsibility for online safety as part of the safeguarding role. The DSL will:

- understand the filtering and monitoring systems and processes in place;
- work with the Headteacher, Computing Lead/IT support and Proprietary Body to review provision;
- ensure online safety incidents and safeguarding alerts are reviewed, recorded and responded to appropriately;
- manage safeguarding concerns in line with the Child Protection and Safeguarding Policy;
- liaise with children's social care, police, local authority, Prevent partners or other agencies when necessary;
- ensure staff receive appropriate online safety and filtering/monitoring updates;
- provide reports and assurance to the Headteacher and Proprietary Body.

4.4 Computing Lead / IT support

- maintain secure ICT systems and appropriate technical controls;
- support the configuration and review of filtering and monitoring;
- ensure operating systems, security software and relevant protections are maintained;
- support investigation of technical issues while preserving safeguarding evidence and confidentiality;
- report safeguarding concerns immediately to the DSL rather than treating them solely as technical issues.

4.5 All staff, agency staff, contractors and volunteers

- read and follow this policy and relevant acceptable use requirements;
- maintain professional curiosity and an attitude that online harm could happen here;
- understand their role in filtering and monitoring, including that technical systems do not replace active supervision;
- report concerns, incidents, accidental access and suspected system weaknesses promptly;
- respond to disclosures calmly, preserve evidence where appropriate and follow safeguarding procedures;
- model safe, respectful and responsible use of technology.

5. Filtering and monitoring

MVFS uses Senso as its filtering and monitoring system across school. Filtering is preventative: it aims to block access to illegal, inappropriate or potentially harmful content. Monitoring is reactive: it identifies activity that may require review or safeguarding action. The school recognises that no technical system is 100% effective and that filtering and monitoring must operate alongside supervision, curriculum teaching, professional curiosity and safeguarding procedures.

- identify and assign roles and responsibilities for filtering and monitoring;
- review filtering and monitoring provision at least annually and after significant changes or serious incidents;
- involve senior leadership, the DSL, IT support and the responsible member of the Proprietary Body in the annual review;
- record the review, identified gaps, decisions and actions;
- consider the pupil risk profile, including age, SEND/SEMH, communication needs, vulnerabilities and patterns of online harm;
- block harmful and inappropriate content without unreasonably impacting teaching and learning;
- maintain effective monitoring strategies and test that systems are operating as intended;
- understand the coverage and limitations of Senso, including devices, users, networks, off-site use where applicable, encrypted/dynamic content and AI-generated content;
- review safeguarding implications before introducing generative AI products or other significant new technologies.

5.1 Alerts, access and escalation

Senso alerts will be reviewed by authorised staff in accordance with the school's agreed safeguarding arrangements. Safeguarding alerts will be triaged according to risk and escalated to the DSL/deputy DSL without avoidable delay. Relevant information will be recorded in the school's safeguarding system in line with normal safeguarding record-keeping procedures. Access to monitoring information will be limited to staff who require it for their role.

Important: A technical alert is information to be assessed, not a safeguarding conclusion. Staff must apply professional judgement and consider context, false positives, the pupil's needs and any wider safeguarding information.

6. Artificial intelligence and emerging technology

MVFS recognises the educational benefits of artificial intelligence (AI) while also recognising risks relating to inaccurate content, bias, privacy, manipulation, harmful content, deepfakes, impersonation, sexualised imagery, over-reliance and inappropriate interaction with AI systems.

- AI tools used with pupils must be appropriate for the intended educational purpose and considered in light of age, developmental level, SEND and safeguarding needs;
- the school will assess safeguarding, privacy, security and filtering/monitoring implications before introducing pupil-facing generative AI products;
- staff must use only school-approved systems for school work where approval is required and must follow data-protection requirements;

- staff must not enter confidential safeguarding information, passwords, or personal/special-category pupil information into unapproved public AI tools;
- AI outputs must be checked for accuracy, bias, suitability and safeguarding concerns;
- AI must not replace professional safeguarding judgement, assessment of a disclosure, or decisions that require accountable human oversight;
- pupils will be taught that AI-generated text, images, audio and video can be convincing but inaccurate or deliberately deceptive;
- concerns involving AI-generated sexual imagery, deepfakes, impersonation, grooming or harassment will be treated as safeguarding concerns and escalated accordingly.

7. Online safety curriculum

Online safety is embedded within MVFS's bespoke Computing Curriculum, particularly through the progressive Digital Wellbeing strand, and is reinforced through PSHE/RSHE, Protective Behaviours and wider safeguarding education. The Computing Curriculum is organised as a two-year cycle and through Stages 1, 2 and 3, enabling teaching to be matched to pupils' developmental understanding and learning needs rather than relying solely on chronological age. This reflects the needs of pupils at MVFS, including pupils who may have experienced significant disruption to previous education and who may be working at different developmental and academic levels.

- Teaching progresses from fundamental concepts including safe use of technology, personal and private information, trusted adults, age restrictions, recognising that online information may not be true, responding safely to unknown adults and reporting worries;
- as pupils develop, teaching extends to digital wellbeing, online relationships, digital footprints, cyberbullying, harmful content and contact, reliability of online information, targeted and ranked content, misinformation, requests for personal information or images, and managing online pressure;
- at the later stage, pupils develop their understanding of privacy and personal boundaries, online harassment and trolling, sharing images, commercial use of data, reliability of sources, age restrictions, online gaming, digital citizenship and strategies for responding to harmful content, contact or pressure;
- the curriculum also supports pupils to understand the importance of balancing time online with other activities and to consider the positive and negative effects of the internet and social media;
- emerging risks, including artificial intelligence, AI-generated content, deepfakes, scams, persuasive or manipulative content, algorithms and targeted content, harmful online attitudes and emerging social-media trends, will be incorporated into Digital Wellbeing, PSHE/RSHE, Protective Behaviours and safeguarding education where developmentally appropriate, rather than being taught in isolation;
- teaching will be adapted to pupils' communication, cognitive, SEMH and SEND needs, using approaches such as visual supports, repetition, concrete examples, social stories, adult scaffolding and Protective Behaviours language;
- the Computing Progression Map and related curriculum planning will be reviewed periodically so that online safety education remains responsive to emerging technology, safeguarding risks and statutory expectations.

Teaching will use current, age-appropriate examples without unnecessarily exposing pupils to harmful material. Where a topic could be distressing or triggering, staff will consider the needs and known experiences of the pupils involved before teaching it.

8. Supporting pupils with SEND, SEMH and additional vulnerabilities

MVFS recognises that some pupils may experience increased online vulnerability or may need additional support to interpret digital interactions, recognise manipulation, manage impulses, understand privacy, generalise rules or communicate a concern. Expectations will therefore be taught according to pupils' developmental understanding and communication needs, not chronological age alone.

- visual supports, social stories, concrete examples and repeated teaching;
- adult scaffolding and checking of understanding;
- Protective Behaviours language and clear help-seeking scripts;
- emotion coaching and regulation strategies following upsetting online experiences;

- careful preparation for topics involving grooming, sexual content, peer pressure or other potentially triggering material;
- individual or small-group teaching where whole-class delivery is not suitable;
- liaison with parents/carers and relevant professionals where additional consistency is needed.

Support will remain strengths-based and will not reduce a pupil's right to privacy, participation, respectful relationships or access to appropriate technology.

9. Child-on-child online abuse and cyberbullying

Child-on-child abuse can occur online and offline and may include cyberbullying, prejudice-based or discriminatory abuse, harassment, sexual violence or sexual harassment, coercion, abuse within intimate personal relationships, non-consensual image sharing, harmful group-chat behaviour, initiation/hazing behaviours and technology-facilitated abuse. Such behaviour is unacceptable and will not be dismissed as banter, part of growing up or an inevitable feature of online life.

Cyberbullying may involve repeated intentional harm through social media, messaging, gaming, images, video or other digital services. The school will teach pupils how to report concerns affecting themselves or others and will respond in line with safeguarding, Behaviour & Regulation and Anti-Bullying/Incidents of Hate procedures.

10. Reporting and responding to concerns

Any member of staff who becomes aware of an online safety concern must consider whether it is a safeguarding matter and follow the Child Protection and Safeguarding Policy. The response will be proportionate to the nature, seriousness, context and impact of the incident and to the needs of the pupils involved.

- ensure immediate safety and provide appropriate reassurance/support;
- do not promise confidentiality;
- avoid unnecessary viewing, forwarding, copying or downloading of harmful material;
- preserve relevant evidence where safe and lawful to do so;
- report promptly to the DSL/deputy DSL and record the concern in accordance with school procedures;
- consider whether parents/carers should be informed, taking account of safeguarding risk;
- consider referrals or reports to children's social care, police, Prevent, CEOP or other appropriate agencies;
- consider support for victims, alleged perpetrators and other affected pupils;
- review whether the incident indicates a weakness in supervision, curriculum, filtering/monitoring or other systems.

Misuse by staff will be managed under the Staff Code of Conduct, disciplinary and safeguarding procedures as appropriate. Allegations or concerns about adults working with children will be managed in accordance with the school's safeguarding procedures, including referral to the LADO where applicable.

11. Searching devices and harmful or illegal content

Any search, screening, confiscation or examination of a pupil device will be undertaken only in accordance with current DfE guidance, school procedures and the law. Staff should involve the DSL/SLT where the concern may be a safeguarding or criminal matter.

Nudes, semi-nudes and potentially illegal imagery: Staff must not routinely view, copy, print, forward or share such imagery. If a member of staff believes a device may contain a nude or semi-nude image, child sexual abuse material, AI-generated sexual imagery or other potentially illegal content, they must report this immediately to the DSL and follow current DfE/UKCIS guidance. Decisions about viewing, securing evidence, confiscation and police involvement will be made by the appropriate safeguarding lead in line with that guidance.

12. Mobile phones and personal devices

Pupils may bring a mobile phone or personal device to school where this is required for transport or agreed circumstances, but they are not permitted to use it during the school day unless specifically authorised by a member of staff for an agreed purpose. Devices will be stored/managed in accordance with school arrangements.

Unauthorised use may result in proportionate action under the Behaviour & Regulation Policy and, where appropriate, confiscation in line with current guidance. Any safeguarding concern arising from a personal device will be referred to the DSL.

13. Staff use of technology and work devices

- keep work devices secure and comply with the school's current password, authentication and cyber-security requirements, including multi-factor authentication where implemented;
- lock devices when unattended and prevent unauthorised access by family members or others;
- install updates and security patches in accordance with school/IT requirements;
- use approved systems for storing and sharing school information;
- not use school systems or devices to access, create or share inappropriate or unlawful material;
- not use personal accounts or unapproved platforms to communicate confidential pupil information;
- follow school requirements for photographs, recordings, social media and communication with pupils/parents;
- report loss, theft, suspected compromise, phishing, malware or other security concerns promptly.

Work devices are provided for professional use. Limited incidental use, if permitted by school arrangements, must never compromise safeguarding, confidentiality, security or professional standards.

14. Working with parents and carers

The school will work in partnership with parents/carers to support safe technology use. This may include information through the school website, letters, workshops, individual support and signposting to trusted organisations.

Parents/carers will be informed, in accessible terms, about:

- the school's approach to filtering and monitoring;
- the online services and technology pupils may be asked to use for learning;
- key online safety themes being taught;
- how to report a concern to school;
- ways to support safe, respectful and developmentally appropriate use at home.

Where an online incident occurs outside school but affects a pupil's safety, wellbeing, relationships or ability to access education, the school may take safeguarding and pastoral action even where the activity did not take place on school systems.

15. Data protection, privacy and cyber security

Filtering and monitoring involve the processing of information about users. MVFS will ensure that this processing is lawful, necessary, proportionate and appropriately secured in accordance with its data-protection arrangements.

- access to monitoring information is restricted to authorised staff with a legitimate role-based need;
- privacy notices and other relevant information explain monitoring where required;
- retention and deletion arrangements are proportionate and consistent with safeguarding and data-protection requirements;
- a Data Protection Impact Assessment (DPIA) will be completed where required before introducing a new monitoring system or making a significant change likely to create high privacy risk;
- school cyber-security arrangements will address accounts and access, malware protection, updates, backups, incident reporting and other current DfE/NCSC requirements;
- suspected data breaches or cyber incidents will be reported immediately through school procedures.

16. Training

All new staff will receive appropriate online safety training as part of induction. All staff will receive safeguarding updates at least annually and additional updates as required. Training will include, as appropriate:

- the role of technology in safeguarding and wellbeing concerns;
- child-on-child abuse online, grooming, exploitation, harmful image sharing and online sexual harassment;
- filtering and monitoring expectations, including what staff must do when a concern or system weakness is identified;
- AI, deepfakes, scams, misinformation and emerging technology risks;
- how SEND/SEMH and other vulnerabilities may affect online risk and teaching;
- reporting, recording, preserving evidence and escalation routes;
- professional use of technology, confidentiality and data protection.

The DSL and deputies will maintain safeguarding knowledge and skills in accordance with KCSIE requirements. The Proprietary Body will receive appropriate safeguarding training, including online safety and filtering/monitoring responsibilities. Volunteers will receive training proportionate to their role.

17. Monitoring, review and annual risk assessment

The Headteacher and DSL will review this policy at least annually and sooner where legislation, statutory guidance, technology, school systems or the school's risk profile changes materially. The policy will be shared with the Proprietary Body for approval/oversight.

The review will be informed by an annual online safety risk assessment and the annual filtering and monitoring review. These will consider, where relevant: incidents and safeguarding trends; pupil voice; curriculum coverage; staff confidence and training; system testing; emerging technologies; AI; SEND/SEMH needs; parent concerns; device/network changes; and lessons learned from incidents. Actions will be recorded and followed up.

18. Links with other policies

- Child Protection and Safeguarding Policy
- Behaviour & Regulation Policy
- Anti-Bullying / Incidents of Hate Policy
- Staff Code of Conduct and disciplinary procedures
- Data Protection Policy and privacy notices
- Complaints Procedure
- Computing / curriculum progression documents
- Relationships Education / RSHE Policy
- Mobile phone / device procedures where separate
- Cyber-security and business continuity arrangements where separate

Appendix 1: Stage 1 acceptable use agreement

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR PUPILS AND PARENTS/CARERS

Name of pupil:

When I use the school's ICT systems (like computers) and get onto the internet in school I will:

- Ask a teacher or adult if I can do so before using them
- Only use websites that a teacher or adult has told me or allowed me to use
- Tell the adults in class immediately if:
 - I click on a website by mistake
 - I receive messages from people I don't know
 - I find anything that may upset or harm me or my friends
- Use school computers for school learning only
- Be kind to others and not upset or be rude to them
- Look after the school ICT equipment and tell a teacher straight away if something is broken or not working properly
- Only use the username and password I have been given
- Try my hardest to remember my username and password
- Never share my password with anyone, including my friends.
- Never give my personal information (my name, address or telephone numbers) to anyone without the permission of my teacher or parent/carer
- Save my work on the school network
- Check with my teacher before I print anything
- Log off or shut down a computer when I have finished using it

I agree that the school will monitor the websites I visit and that there will be consequences if I don't follow the expectations.

Signed (pupil):

Date:

Parent/carer agreement: I agree that my child can use the school's ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for pupils using the school's ICT systems and internet, and will make sure my child understands these.

Signed (parent/carer):

Date:

Appendix 2: Stage 2 & 3 acceptable use agreement

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR PUPILS AND PARENTS/CARERS

Name of pupil:

I will read and follow the rules in the acceptable use agreement policy.

When I use the school's ICT systems (like computers) and get onto the internet in school I will:

- Always use the school's ICT systems and the internet responsibly and for educational purposes only
- Only use them when a teacher is present, or with a teacher's permission
- Keep my usernames and passwords safe and not share these with others
- Keep my private information safe at all times and not give my name, address or telephone number to anyone without the permission of my teacher or parent/carer
- Tell a teacher or support staff immediately if I find any material which might upset, distress or harm me or others
- Always log off or shut down a computer when I've finished working on it

I will not:

- Access any inappropriate websites including: social networking sites, chat rooms and gaming sites unless my teacher has expressly allowed this as part of a learning activity
- Open any attachments in emails, or follow any links in emails, without first checking with a teacher
- Use any inappropriate language when communicating online, including in emails
- Create, link to or post any material that is pornographic, offensive, obscene or otherwise inappropriate
- Log in to the school's network using someone else's details
- Arrange to meet anyone offline without first consulting my parent/carer, or without adult supervision

If I bring a personal mobile phone or other personal electronic device into school:

- I will not use it during school time, without a teacher's permission
- I will use it responsibly, and will not access any inappropriate websites or other inappropriate material or use inappropriate language when communicating online

I agree that the school will monitor the websites I visit and that there will be consequences if I don't follow the expectations.

Signed (pupil):

Date:

Parent/carer's agreement: I agree that my child can use the school's ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for pupils using the school's ICT systems and internet, and for using personal electronic devices in school, and will make sure my child understands these.

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR PUPILS AND PARENTS/CARERS

Signed (parent/carer):

Date:

Appendix 3: Acceptable use agreement - staff, Proprietary Body, volunteers and visitors

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR STAFF, GOVERNORS, VOLUNTEERS AND VISITORS

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR STAFF, GOVERNORS, VOLUNTEERS AND VISITORS

Name of staff member/governor/volunteer/visitor:

When using the school's ICT systems and accessing the internet in school, or outside school on a work device (if applicable), I will not:

- Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature (or create, share, link to or send such material)
- Use them in any way which could harm the school's reputation
- Access social networking sites or chat rooms
- Use any improper language when communicating online, including in emails or other messaging services
- Install any unauthorised software, or connect unauthorised hardware or devices to the school's network
- Share my password with others or log in to the school's network using someone else's details
- Take photographs of pupils without checking with teachers first
- Share confidential information about the school, its pupils or staff, or other members of the community
- Access, modify or share data I'm not authorised to access, modify or share
- Promote private businesses, unless that business is directly related to the school

I will only use the school's ICT systems and access the internet in school, or outside school on a work device, for educational purposes or for the purpose of fulfilling the duties of my role.

I agree that the school will monitor the websites I visit and my use of the school's ICT facilities and systems.

I will take all reasonable steps to ensure that work devices are secure and password-protected when using them outside school, and keep all data securely stored in accordance with this policy and the school's data protection policy.

I will let the designated safeguarding lead (DSL) and ICT manager know if a pupil informs me they have found any material which might upset, distress or harm them or others, and will also do so if I encounter any such material.

I will always use the school's ICT systems and internet responsibly, and ensure that pupils in my care do so too.

Signed (staff member/governor/volunteer/visitor):

Date:

Appendix 4: Online safety training needs self-audit

Statement	Yes / No	Comments / training need
I know who has lead responsibility for online safety and filtering/monitoring.		
I understand my role in filtering and monitoring and what to do if I identify a concern or weakness.		
I know how pupils may experience child-on-child abuse online.		
I know what to do if a pupil reports harmful content, grooming, harassment or image sharing.		
I understand the additional online vulnerabilities that may affect pupils with SEND/SEMH.		
I understand school expectations for AI use, confidential information and data protection.		
I know how to report a phishing, malware, lost-device or data-security concern.		
I am familiar with the acceptable use requirements relevant to my role.		

Name: _____ Date: _____

Appendix 5: Online safety incident record

Date/time	
Pupil(s)/person(s) involved	
Reported by	
Type of concern / 4C category	
Summary of concern	
Immediate action taken	
DSL review / safeguarding action	
External referral/report if applicable	
Follow-up / lessons learned (including filtering, monitoring or curriculum action)	

Review sources (September 2026): Keeping Children Safe in Education 2026; DfE Filtering and Monitoring: Core Standard (updated 25 August 2026); revised RSHE statutory guidance in force from 1 September 2026; DfE Generative AI: Product Safety Standards; and the source MVFS policy reviewed August 2026.