Online Safety Policy

Forest Skies Federation

Written to reflect Keeping Children Safe in Education 2026, in force from 1 September 2026.

Approved by:	COG Mr Matthew Davies Miss Naomi Haughton Miss Joanne Bingwa	**Date:** 29.09.2026
Last reviewed on:	September 2026	
Next review due by:	September 2027	

Policy title	Online Safety Policy
Scope	Forest Skies Federation
Version	1.0
Supersedes	[Insert title and date of previous policy, if any]
Written by	M.Davies/ N.Haughton/ J.Bingwa
Approved by	Full Governing Body
Date approved	29.09.2026
Date of next review	September 2027
Statutory review cycle	Annual. Reviewed each September against the current edition of Keeping Children Safe in Education.

Contents

1. Aims

2. Scope

3. Legislation and guidance

4. How we describe online risk: the four Cs

5. Roles and responsibilities

6. Filtering and monitoring

7. Artificial intelligence

8. Mobile phones and personal devices

9. Teaching pupils about online safety

10. Working with parents and carers

11. Staff training

12. Cyber-bullying and online child-on-child abuse

13. Nudes and semi-nudes, including AI-generated images

14. Searching, screening and examining electronic devices

15. Images of pupils and staff

16. Remote and blended learning

17. Data protection and cyber security

18. Responding to online safety concerns

19. Responding to misuse

20. Monitoring, evaluation and review

Appendix A Online safety incident response — decision route

Appendix B Filtering and monitoring annual review record

Appendix C Staff online safety self-audit

Appendix D Local systems annex

Appendix E Related policies and agreements

1. Aims

Forest Skies Federation aims to:

- keep pupils, staff, volunteers, governors and visitors safe when they are using technology on our premises, on our systems and on our devices;
- teach pupils to recognise online risk and to act on it, so that they are safer when they are not with us;
- operate filtering and monitoring systems that are effective, reviewed annually and evidenced;
- identify, record, escalate and resolve online safety incidents through a single, understood route;
- work with parents and carers on the risks children meet at home, which are greater in number and less easily controlled than those they meet in school;
- adopt new technology, including generative artificial intelligence, only where the safeguarding and data protection position has been considered first.

POSITION

Filtering and monitoring reduce risk on our network. They do not remove it, and they have no effect at all on the device a child uses at home. The most significant online risks our pupils face are outside our filtering. Our teaching, our reporting culture and our work with parents are therefore not supplementary to this policy — they are the substance of it.

2. Scope

This policy applies to all pupils on roll, all staff (including supply staff, agency staff and contractors), all volunteers, all governors and all visitors who use the school's systems, network, devices or internet connection.

It applies:

- on the school site, at all times;
- on educational visits, residentials and off-site activities;
- to the use of school-owned devices anywhere, including at a member of staff's home;
- to remote and blended learning delivered by the school;
- to conduct outside school where that conduct affects the safety, wellbeing or education of a pupil at this school, or the reputation or safe operation of the school.

3. Legislation and guidance

This policy is based on the following statutory guidance and legislation. Where a document is revised, this policy is read as referring to the current version.

3.1 Statutory guidance

- **Keeping Children Safe in Education (Department for Education, 2026)** — in force from 1 September 2026. Part One is read in full by all staff; Annex A was withdrawn in the 2026 edition.
- **Working Together to Safeguard Children (2023)** — the multi-agency safeguarding framework.
- **Mobile phones in schools (Department for Education)** — given force of law by section 36 of the Children's Wellbeing and Schools Act 2026. Schools must have regard to it.

- **Searching, screening and confiscation: advice for schools (Department for Education)**.
- **The Prevent duty guidance (2023)** — including the requirement that the Prevent risk assessment informs filtering decisions.
- **Sharing nudes and semi-nudes: advice for education settings (UK Council for Internet Safety)**.
- **Behaviour in schools (Department for Education)**.

3.2 Standards and non-statutory guidance

- **Filtering and monitoring standards for schools and colleges (Department for Education)** — the benchmark against which our provision is assessed.
- **Cyber security standards for schools and colleges (Department for Education)**.
- **Generative AI product safety guidance for education (Department for Education)** — referenced by Keeping Children Safe in Education 2026 as the basis for applying filtering and monitoring requirements to generative AI.
- **Meeting digital and technology standards in schools and colleges (Department for Education)**.

3.3 Legislation

- Education Act 1996 (as amended)
- Education and Inspections Act 2006
- Education Act 2011
- Equality Act 2010
- Children and Families Act 2014
- Data Protection Act 2018 and the UK General Data Protection Regulation
- Computer Misuse Act 1990
- Protection of Children Act 1978 and the Sexual Offences Act 2003
- Malicious Communications Act 1988 and the Communications Act 2003
- Online Safety Act 2023
- Children's Wellbeing and Schools Act 2026
- Crime and Policing Act 2026 (volunteer vetting and regulated activity)

The National Curriculum computing programmes of study and the statutory Relationships Education and Health Education requirements also shape the taught content described at section 9.

4. How we describe online risk: the four Cs

Keeping Children Safe in Education groups online risk under four headings. We use the same headings in staff training, in incident recording and in this policy, so that a concern is categorised the same way by everyone who handles it.

Category	What it covers	Examples relevant to a junior school
Content	Being exposed to illegal, inappropriate or harmful material.	Pornography; violence and gore; content promoting self-harm, suicide or disordered eating; racist, misogynistic or extremist material; disinformation, misinformation and conspiracy theories, which Keeping Children Safe in Education 2026 added to this category.
Contact	Being subjected to harmful online interaction with another user.	Adults seeking contact with children for sexual or exploitative purposes; peer pressure; commercial advertising directed at children; interaction with generative AI systems that simulate human conversation, which Keeping Children Safe in Education 2026 added to this category.
Conduct	Behaviour by a child, online, that causes harm to themselves or others.	Making, sending or receiving nudes and semi-nudes, including images that are digitally altered or wholly AI-generated; cyber-bullying; sharing another child's image or personal information; deliberately accessing prohibited material.
Commerce	Being exposed to financial harm.	In-game purchasing and loot boxes; gambling mechanics in games; phishing; scams; financial and sextortion-style scams.

NOTE FOR STAFF

The four Cs are a sorting tool, not a threshold. A concern is reported to the Designated Safeguarding Lead because it concerns you, not because you have successfully categorised it. Categorise afterwards, or let the DSL do it.

5. Roles and responsibilities

5.1 The Governing Body

The Governing Body of the Forest Skies Federation has overall responsibility for online safety. It will:

- approve this policy and review it annually;
- ensure that appropriate filtering and monitoring systems are in place, that their effectiveness is reviewed at least once every academic year, and that the school can demonstrate those reviews have taken place;
- receive the completed annual filtering and monitoring review record (Appendix B) and minute its consideration;
- ensure that the roles and responsibilities for filtering and monitoring set out in this policy are reflected in the relevant job descriptions;
- ensure all governors receive online safety training as part of their safeguarding training, and that they understand the risks specific to primary-aged children;
- ensure all governors agree to and comply with the Acceptable Use Agreement;

- receive a termly online safety report from the Designated Safeguarding Lead covering incident volumes, themes, curriculum coverage and any filtering breaches.

The Governing Body has appointed Helen Pennington as the link governor for safeguarding and online safety. The link governor meets the Designated Safeguarding Lead at least termly and reports to the full Governing Body.

5.2 The Headteacher

The Headteacher is responsible for ensuring that this policy is understood and implemented consistently, that staff are trained, that adequate resourcing is in place for filtering and monitoring provision, and that online safety is treated as a whole-school safeguarding responsibility rather than a technical one.

5.3 The senior leader responsible for filtering and monitoring

Keeping Children Safe in Education 2026 requires that a member of the senior leadership team is responsible for reviews of filtering and monitoring systems, supported by the Designated Safeguarding Lead and by IT staff or providers.

At Forest Skies Federation this is the Headteacher:

- leading the annual review of the effectiveness of filtering and monitoring, using Appendix B;
- commissioning and recording the practical checks that sit behind that review — that filtering works as intended across every type of internet-connected device the school uses, in every location where those devices are used;
- ensuring the outcome of the review, and any actions arising, are reported to the Governing Body;
- ensuring that any change to systems, devices, providers or user groups triggers a re-check rather than waiting for the annual cycle;
- maintaining the record of blocked and unblocked site requests and the reasons for each decision.

FREQUENTLY CONFUSED

This is not the same role as the Designated Safeguarding Lead, the Computing Lead or the IT provider, although one person may hold more than one of them at this school. If the same person holds all of them, the school has no internal check on filtering and should say so openly to governors and arrange external assurance.

5.4 The Designated Safeguarding Lead

The Designated Safeguarding Lead, named in the Safeguarding and Child Protection Policy, takes lead responsibility for online safety. This includes:

- understanding the filtering and monitoring systems in place, how they are operated, what they can and cannot detect, and how alerts reach a person;
- supporting the senior leader named at 5.3 in the annual review;
- ensuring all online safety concerns are recorded on CPOMS and responded to in line with the Safeguarding and Child Protection Policy;
- triaging incidents, deciding thresholds, and making referrals to children's social care, the police, the Internet Watch Foundation or the Child Exploitation and Online Protection command as appropriate;
- leading and updating staff training on online safety, including on generative AI;

- advising on the online safety implications of any new system, platform, device or application before it is adopted;
- reporting to the Headteacher and Governing Body termly.

This responsibility is reflected in the Designated Safeguarding Lead's job description, as Keeping Children Safe in Education 2026 requires.

5.5 The Computing Lead

The Computing Lead is responsible for the taught online safety curriculum: its sequence, its coverage across year groups, the resources used, and assurance that what is planned is actually taught. The Computing Lead works with the Designated Safeguarding Lead to ensure the curriculum responds to the concerns actually being logged in this school.

5.6 The IT support provider

Ark is responsible for the technical operation of the network, devices, filtering and monitoring systems. The provider is contractually required to:

- maintain filtering and monitoring provision that meets the Department for Education's filtering and monitoring standards;
- apply security updates and patches, and maintain anti-malware protection;
- support the annual review by supplying evidence of system performance and check results;
- escalate technical faults affecting filtering or monitoring to the senior leader named at 5.3 on the same working day.

ACCOUNTABILITY

Filtering and monitoring is a school responsibility that cannot be contracted out. The provider operates the system; the school assures itself that the system works. Where a provider supplies assurance about its own product, that is a supplier statement, not a school review.

5.7 All staff and volunteers

All staff, volunteers, supply staff, agency staff and contractors are responsible for:

- reading and following this policy and the Staff ICT and AI Acceptable Use Agreement;
- reporting any online safety concern to the Designated Safeguarding Lead on the day it arises, without carrying out their own investigation first;
- reporting any filtering breach — including accidental access to inappropriate material by an adult — to the senior leader named at 5.3 and the Designated Safeguarding Lead;
- supervising pupils' use of technology actively, in the room, rather than relying on monitoring software;
- modelling safe and professional online conduct;
- never leaving a device logged in and unattended, and never sharing credentials.

5.8 Pupils

Pupils are expected to follow the Pupil Acceptable Use Agreement appropriate to their year group, which they and their parents sign annually. Pupils are taught that they will not be in trouble for reporting

something that has worried them online, including where they broke a rule to get there. This is stated to pupils explicitly and repeatedly, and staff must honour it.

5.9 Parents and carers

Parents and carers are expected to:

- read this policy and sign the Pupil Acceptable Use Agreement with their child;
- support the school's mobile phone position (section 8);
- supervise their child's use of devices, games, apps and platforms at home, including checking age ratings;
- contact the school if they have a concern about their child's online experience, whether it arose at school or at home.

5.10 Visitors, contractors and community users

Visitors who use the school network or devices will be made aware of this policy and asked to agree to the Acceptable Use Agreement. Visitors are not given access to pupil-facing systems. Where school premises are let to an external organisation, the letting agreement sets out that organisation's own safeguarding responsibilities, and allegations arising from a letting are handled under the Safeguarding and Child Protection Policy.

6. Filtering and monitoring

6.1 Our systems

The school operates:

- **Filtering:** — restricts access to harmful and inappropriate content across the school network and on school devices.
- **Monitoring:** — records and flags user activity, generating alerts on defined keywords, phrases and behaviours.

Full technical detail, including which device types and locations are covered and who receives alerts, is held in Appendix D and is updated whenever provision changes.

6.2 What our systems cover

Filtering and monitoring apply to all school-owned devices used on site, and to school-owned devices used off site where technically possible. Coverage details, including any known gaps, are recorded in Appendix D. Known gaps are stated to the Governing Body rather than left unmentioned.

6.3 The annual review

The effectiveness of filtering and monitoring is reviewed at least once every academic year, and more often where systems, providers, devices or user groups change. The review is led by the senior leader named at 5.3, supported by the Designated Safeguarding Lead and the IT provider, and is recorded using Appendix B.

The review considers, as a minimum:

- whether filtering blocks what it is intended to block, tested on each type of internet-connected device in each location where those devices are used;
- whether monitoring alerts reach a named person, and how quickly, including outside the school day;
- how many alerts were generated, how many were acted on, and what happened to those that were not;
- whether the provision meets the Department for Education's filtering and monitoring standards;
- whether the provision addresses the risks identified in the school's Prevent risk assessment;
- whether the provision can address real-time, dynamic, personalised and AI-generated content (see section 7.4);
- whether any pupil group — for example pupils with special educational needs using assistive technology — is subject to filtering that is either too permissive or so restrictive that it obstructs their education.

The completed record is presented to the Governing Body and retained. The school must be able to demonstrate that these reviews have taken place; the record is that demonstration.

6.4 Responding to a monitoring alert

Alerts are received by the Headteacher: On receipt:

Step	Action	Timescale
1	The alert is reviewed by the receiving member of staff and, if it concerns a pupil, passed to the Designated Safeguarding Lead.	Same school day
2	The Designated Safeguarding Lead determines whether the alert indicates a safeguarding concern, a behaviour matter, a technical false positive, or a combination.	Same school day
3	Safeguarding concerns are recorded and progressed under the Safeguarding and Child Protection Policy. Behaviour matters are progressed under the Behaviour Policy.	Same school day
4	False positives and filtering gaps are logged and passed to the senior leader named at 5.3 for adjustment.	Within 2 school days
5	Repeat themes are reported to the Computing Lead so the curriculum can respond.	Termly

Alerts are never deleted, dismissed or resolved without a record of who reviewed them and what decision was taken.

6.5 Requests to block or unblock a site

Staff may request that a site be blocked or unblocked. Requests are made to the headteacher, considered against the educational purpose and the risk, and recorded with the decision and its reason. Staff do not circumvent filtering, use personal hotspots to reach blocked content, or ask pupils to access content from home that is blocked at school.

6.6 What filtering and monitoring cannot do

Staff and governors should understand the limits of these systems:

- they operate on school devices and the school network, and have no effect on a child's own device on mobile data or at home;
- URL and DNS-based filtering cannot see inside encrypted, dynamically generated or AI-generated content that never appears on a blocklisted page;
- monitoring generates alerts; it does not generate responses. An unread alert offers no protection at all;
- a system that has never been tested is a system whose effectiveness is unknown, not a system that works.

7. Artificial intelligence

Generative artificial intelligence is now addressed directly in Keeping Children Safe in Education. This section sets out the school's position.

7.1 Staff use

Staff use of generative AI is governed by the Staff ICT and AI Acceptable Use Agreement, which all staff sign annually. In summary:

- only tools approved by the school may be used for school work. The approved list, and the data protection impact assessment completed for each.
- no formal name of any pupil, parent or member of staff may be entered into any generative AI tool, and neither may any other information from which an individual could be identified;
- AI output is a draft. The member of staff remains professionally accountable for anything they send, publish or act on;
- AI is not used to make or to substantially inform decisions about individual children, including assessment, admissions, exclusions or safeguarding judgements.

7.2 Pupil use

Pupils do not use open generative AI tools independently. Where AI is used, it is used by the teacher, on the board, with the class, as a taught object rather than a pupil tool.

Where any AI-enabled product is used with pupils, the school will first check it against the Department for Education's generative AI product safety guidance, complete a data protection impact assessment, and confirm the age requirements in the supplier's terms. Many general-purpose AI tools require users to be 13 or 18; no pupil at this school meets either threshold.

7.3 AI as a safeguarding risk

Staff should be alert to three specific risks:

- **Simulated relationships.** Keeping Children Safe in Education 2026 treats interaction with AI systems that simulate human conversation as a contact risk. Companion and character chatbots are marketed to children, are not age-appropriate, and can normalise disclosure of personal information or reinforce distress.
- **AI-generated imagery.** Images that are digitally altered or wholly AI-generated are within the definition of nudes and semi-nudes (see section 13). Photographs of children taken from school websites and social media have been used to generate such images. Section 15 sets out our response.
- **Plausible falsehood.** AI output is fluent regardless of accuracy. Pupils are taught to check claims against sources, and staff should assume that a confidently written answer may still be wrong.

7.4 AI and our filtering

Filtering that operates on web addresses cannot reliably assess content generated in real time by an AI system. Whether our provision can address AI-generated content is a specific question in the annual review at Appendix B, and is answered rather than assumed.

8. Mobile phones and personal devices

Section 36 of the Children's Wellbeing and Schools Act 2026 requires schools to have regard to the Department for Education's guidance on mobile phones in schools. Keeping Children Safe in Education 2026 sets the expectation that schools are mobile phone-free environments by default, with anything other than that by exception only.

8.1 The school's position

Forest Skies Federation is a mobile phone-free federation. Pupils do not have access to a mobile phone or any device with similar functionality at any point between arriving on site and leaving site, including lessons, the time between lessons, breaktime and lunchtime.

"Similar functionality" includes any device that can message, call, photograph, record, browse or receive notifications. This includes smart watches, fitness trackers with messaging, tablets, smart glasses and gaming handhelds.

8.2 How this works in practice

No mobile phone devices are allowed on site at all.

8.3 Exceptions

An exception may be agreed in writing by the Headteacher where a phone or device is necessary:

- to meet a pupil's medical needs, under the Children and Families Act 2014 — for example a continuous glucose monitor paired to a phone;
- as a reasonable adjustment for a disabled pupil under the Equality Act 2010;
- as part of an agreed arrangement to support a pupil's specific circumstances, for example a young carer or a pupil who travels a long distance unaccompanied.

Exceptions are recorded, time-limited, reviewed, and set out what the pupil may and may not do with the device. A generalised parental preference is not an exception.

8.4 Contacting your child during the school day

Parents who need to reach their child during the school day contact the school office, which will pass the message on. This is stated to parents each September and on the school website. It is the answer to the most common objection to a phone-free school and should be given before the objection is raised.

8.5 School trips and residentials

Pupils do not take mobile phones on day trips or residential visits.

8.6 Staff personal devices

- Staff personal phones are not used in classrooms or any area where pupils are present, except in an emergency or where a specific arrangement has been agreed with the Headteacher.
- Staff personal phones and personal cameras are never used to photograph or record pupils (see section 15).
- Staff do not communicate with pupils or parents from personal accounts, personal numbers or personal social media.

- Personal devices are not connected to the school's staff or pupil networks. A separate guest network is available where one is provided.

8.7 Visitors and volunteers

Visitors and volunteers are asked not to use mobile phones in areas where pupils are present. This is included in the visitor briefing and the volunteer induction.

9. Teaching pupils about online safety

Online safety is taught through the computing curriculum, through Relationships and Health Education within our RSHE and PSHE provision, through assemblies, and through direct teaching at the point a concern arises.

9.1 Coverage

By the end of Key Stage 2, pupils are taught to:

- use technology safely, respectfully and responsibly;
- recognise acceptable and unacceptable behaviour, online and offline;
- identify a range of ways to report concerns about content and contact, in school and outside it;
- recognise that people online may not be who they say they are, including where the "person" is not a person;
- understand that images and information shared online may be copied, altered and shared further without their agreement, and may be permanent;
- recognise pressure, coercion and manipulation in online interactions with adults and with peers;
- question the reliability of what they read, watch and are shown, including AI-generated content;
- understand the financial mechanics of games and apps, including in-app purchasing and reward loops;
- know that they will not be in trouble for reporting something that has worried them.

9.2 Sequence and responsiveness

The Computing Lead maintains the taught sequence and reviews it annually with the Designated Safeguarding Lead against the concerns actually recorded in this school. A curriculum that does not respond to the school's own incident log is a generic curriculum.

9.3 Pupils who are more vulnerable online

Pupils with special educational needs, pupils with a social worker, children in care and pupils with limited support at home are at greater risk online and are less likely to report. Teaching is adapted rather than simplified, and the Designated Safeguarding Lead and SENDCO agree any additional arrangements. Where a pupil cannot reliably report verbally, an alternative reporting route is agreed and recorded.

10. Working with parents and carers

Keeping Children Safe in Education 2026 reinforces the importance of talking to parents about children's access to online sites when they are away from school. The school will:

- publish this policy on the school website;
- provide parents with a plain-English summary of what the school does and what parents need to do at home;
- cover online safety at the new intake meeting, at parents' evenings and in regular communications;
- signpost parents to independent sources of advice and to the routes for reporting harmful content;
- contact parents directly where a concern about their child's online activity arises, unless doing so would place a child at risk, in which case the Safeguarding and Child Protection Policy applies.

Recommended sources for parents:

- UK Safer Internet Centre — advice for parents and carers
- Internet Matters — age-specific guidance and parental control setup guides
- Childnet International — parent and carer resources
- Thinkuknow (National Crime Agency) — including the report route for concerns about an adult's contact with a child
- Report Harmful Content — for content that is harmful but not illegal
- Internet Watch Foundation — for reporting child sexual abuse imagery

11. Staff training

Who	What	When
All staff and volunteers	Online safety as part of safeguarding induction, including this policy, the four Cs, the reporting route, filtering and monitoring, cyber-bullying, radicalisation and the school's AI position.	On induction, before contact with pupils
All staff and volunteers	Refresher training, plus updates through briefings, bulletins and staff meetings as issues arise.	At least annually, with in-year updates
All staff	Read Part One of Keeping Children Safe in Education in full. Annex A was withdrawn in the 2026 edition, so the condensed version is no longer available.	Annually
Designated Safeguarding Lead and deputies	Child protection and safeguarding training including online safety.	At least every 2 years
Designated Safeguarding Lead and deputies	Update knowledge and skills on online safety, including filtering and monitoring systems and generative AI.	At least annually, and at regular intervals
Senior leader responsible for filtering and monitoring	Training sufficient to lead the annual review and interrogate supplier assurance.	Annually
Governors	Online safety within safeguarding training, including the Governing Body's specific filtering and monitoring duties.	On appointment and at least every 2 years

Staff complete the self-audit at Appendix C annually. Returns are analysed by the Designated Safeguarding Lead and used to plan the following year's training, rather than filed.

12. Cyber-bullying and online child-on-child abuse

12.1 Definition

Cyber-bullying is the repeated, intentional harming of a person or group by another person or group, carried out online, where the relationship involves an imbalance of power. It is one form of child-on-child abuse and is handled as a safeguarding matter as well as a behaviour matter.

Online child-on-child abuse also includes: sharing nudes and semi-nudes; sexual harassment carried out online; the creation or sharing of altered or AI-generated images of another child; coercion; and the deliberate exclusion of a child from online groups. Keeping Children Safe in Education 2026 places increased emphasis on misogyny and its relationship with harmful sexual behaviour; staff should not dismiss this as a secondary-phase issue.

12.2 Prevention

- Pupils are taught what cyber-bullying is, why it happens, what it feels like, and how to report it — including where they are a witness rather than the person targeted.
- Cyber-bullying is addressed in assemblies, in PSHE and at the point of incident.
- Staff and governors receive training on cyber-bullying as part of safeguarding training.
- Parents receive information on the signs, on how to report, and on how to support a child who is affected.

12.3 Response

Incidents are handled under the Behaviour Policy and the Anti-Bullying Policy, with the Safeguarding and Child Protection Policy taking precedence where there is a safeguarding concern. The school will:

- record the incident and support the child who has been harmed;
- take all reasonable steps to contain the spread of any harmful material;
- work with the child who caused the harm, recognising that a child who abuses another child is themselves a safeguarding concern;
- consider whether the matter should be reported to the police, and consult the police where there is any doubt;
- inform parents of both children, unless doing so would place a child at risk.

Staff do not treat online incidents as less serious because they occurred outside school hours or on a home device. The effect on the child in the classroom is the same.

13. Nudes and semi-nudes, including AI-generated images

Keeping Children Safe in Education 2026 uses the term "nudes and semi-nudes" and extends the definition to images that are digitally altered or wholly generated using artificial intelligence, including material sometimes described as deepfakes or deep nudes. All incidents involving the sharing of such images require a safeguarding response, whether the sharing was consensual or not.

STAFF MUST NOT

View, copy, forward, print, share or store the image. Ask the child to show you the image. Ask the child to delete the image. Search for the image on a device. Investigate the circumstances yourself. Any of these can constitute a criminal offence and all of them compromise the response.

13.1 What staff do

If a member of staff becomes aware of any nude or semi-nude image involving a child, they:

- confiscate and secure any device involved, if it is safe and practicable to do so, without looking at its contents;
- report to the Designated Safeguarding Lead immediately — the same day, in person, not by email alone;
- record what they were told or saw, in the words used, as soon as possible;
- tell nobody else.

13.2 What the Designated Safeguarding Lead does

The Designated Safeguarding Lead follows the UK Council for Internet Safety guidance Sharing nudes and semi-nudes: advice for education settings, which sets out when an incident must be referred to the police and children's social care and the limited circumstances in which a school may handle it internally. The Designated Safeguarding Lead will refer immediately where:

- an adult is involved;
- there is reason to believe a child has been coerced, blackmailed or groomed, or there are concerns about their capacity to consent;
- the images show sexual acts, or any child under 13;
- a child is at immediate risk of harm.

The Internet Watch Foundation's Report Remove service is used to seek removal of images of a child from the internet, and the child and their parents are supported through that process.

Given the age of our pupils, a nude or semi-nude image involving a child at this school will almost always meet the threshold for referral. Staff should assume it does.

14. Searching, screening and examining electronic devices

Staff have the power under the Education and Inspections Act 2006 to search for and, where necessary, delete inappropriate images or files on a pupil's electronic device where they have a good reason to do so. Searches are conducted in line with the Department for Education's guidance on searching, screening and confiscation.

14.1 Good reason

A member of staff must reasonably suspect that the data or file has been, or could be, used to:

- cause harm; and/or
- disrupt teaching; and/or
- break any of the school rules.

14.2 Authorisation and conduct

- Only the Headteacher, or a member of staff authorised in writing by the Headteacher, may carry out a search of a device.
- Two members of staff are present, at least one of whom is the same sex as the pupil where practicable.
- The pupil is told why the search is happening and given the opportunity to explain.
- The search is recorded: who, when, why, what was found, what was done, and who was informed.
- Parents are informed, unless doing so would place the child at risk.

14.3 If material is found

The member of staff, together with the Designated Safeguarding Lead or another member of the senior leadership team, decides whether to delete the material, retain it as evidence, or report it to the police. Where the material is, or may be, a nude or semi-nude image of a child, section 13 applies and the device is secured without further examination.

14.4 Complaints

Complaints about a search, or about the deletion of material, are handled under the Complaints Policy.

15. Images of pupils and staff

The misuse of images of children is a rising risk. Photographs taken from school websites and school social media accounts have been used to generate sexualised imagery using AI tools. The UK Safer Internet Centre has issued specific guidance to education settings on this.

15.1 Taking images

- Images of pupils are taken only on school-owned devices. Personal phones and personal cameras are never used.
- Images are transferred to school storage and deleted from the device promptly.
- Images are not stored on personal devices, personal cloud accounts or home computers.

15.2 Publishing images

- Consent is checked against the register before any image is published. This is checked every time, not assumed from a form signed at admission.
- Names are not published alongside images of pupils.
- Images published externally are of a resolution and framing that limits their usefulness for manipulation. Group shots are preferred to close portraits.
- The school reviews what is published about individual children and removes historic content on request.

15.3 Parents and visitors taking images

Parents may take photographs at school events for personal use only. They are asked, at every event and in writing, not to publish images containing other people's children on social media. Where a pupil's circumstances require that no image of them is taken, this is managed discreetly and the arrangement is known to the staff running the event.

16. Remote and blended learning

Where the school provides live remote teaching or online contact with pupils, the following apply. They are also the standards expected of any external provider working with our pupils remotely.

- Only school-provided platforms, accounts and phone numbers are used. Personal accounts are never used.
- Meeting links and identifiers are never shared on public platforms.
- One-to-one sessions do not take place without another adult present. If no adult is available at the pupil's end, a colleague joins the session; if that is not possible, the session does not go ahead.
- Staff and pupils are appropriately dressed, and the setting is an appropriate room — not a bedroom.
- Backgrounds are blurred or neutral, with no identifying features that would reveal a home address or family members.
- Sessions are recorded only where there is a stated purpose, parents have been informed, and the recording is stored securely and deleted to schedule.
- Staff continue to look for signs that a child may be at risk, and report to the Designated Safeguarding Lead exactly as they would in school.
- If an adult uses a session to raise a complaint, staff ask them to contact the school separately. If an adult becomes aggressive or abusive, staff end the session and report it the same day.

Pupils are reminded at the start of any period of remote learning who they can contact for help and how.

17. Data protection and cyber security

The school's obligations under the Data Protection Act 2018 and the UK General Data Protection Regulation are set out in the Data Protection Policy. In relation to online safety:

- a data protection impact assessment is completed before any new system that processes pupil data is adopted, including any AI-enabled system;
- monitoring of users is proportionate, is explained to users in advance through the Acceptable Use Agreements and this policy, and its records are handled as personal data;
- school data is stored on approved school systems only. Personal cloud accounts and unencrypted removable media are not used;
- any device or removable medium holding school data is encrypted;
- credentials are not shared. Multi-factor authentication is enabled where available;
- staff report suspected phishing, ransomware or unauthorised access to [ROLE] immediately, and do not attempt to resolve it themselves;
- the school follows the Department for Education's cyber security standards for schools and colleges, and maintains an incident response plan and offline backups.

A personal data breach is reported internally on the day it is identified so that the Data Protection Officer can assess whether the Information Commissioner's Office must be notified within 72 hours. Delay in internal reporting is the most common cause of a missed deadline.

The school's Data Protection Officer is:

Judicium Education Limited, 5th Floor, 98 Theobalds Road, London, WC1X 8WB

18. Responding to online safety concerns

Any online safety concern — about a pupil, a member of staff, a parent, a visitor or a system — goes to the Designated Safeguarding Lead on the day it arises.

Staff do not:

- decide for themselves whether a concern meets a threshold;
- investigate before reporting;
- promise a child confidentiality;
- contact a parent about a safeguarding concern before speaking to the Designated Safeguarding Lead;
- delay because it is late in the day, because they are not certain, or because the concern arose outside school.

Appendix A sets out the decision route, including for illegal content and for concerns about an adult. Concerns about an adult working at the school are handled under the allegations procedure in the Safeguarding and Child Protection Policy and go to the Headteacher, or to the Chair of Governors and the Local Authority Designated Officer where the concern is about the Headteacher.

19. Responding to misuse

Who	Route	Notes
Pupils	Behaviour Policy, with the Safeguarding and Child Protection Policy taking precedence where there is a safeguarding concern.	The response is proportionate to the incident. A pupil who reports their own rule-breaking in order to report a concern is not sanctioned for the rule-breaking.
Staff and volunteers	Staff Disciplinary Procedure, or the allegations procedure where the concern relates to a risk to children.	Low-level concerns about adult conduct online are recorded and reviewed for patterns, as set out in the Safeguarding and Child Protection Policy.
Parents and carers	Parent/Carer Code of Conduct.	Includes online conduct directed at staff, pupils or the school, and posts on social media naming or depicting pupils or staff.
Visitors and contractors	Access withdrawn; matter referred to their employer where applicable.	

The school will consider in every case whether an incident involving illegal activity or content should be reported to the police, and will consult where there is doubt rather than deciding alone.

20. Monitoring, evaluation and review

- Online safety concerns are recorded on [SAFEGUARDING RECORDING SYSTEM] and analysed termly by the Designated Safeguarding Lead for themes, patterns and gaps.
- The Designated Safeguarding Lead reports termly to the Headteacher and the Governing Body on incident volumes, themes, curriculum coverage, training completion and any filtering breaches.
- The filtering and monitoring review (Appendix B) is completed at least annually and reported to the Governing Body.
- This policy is reviewed annually by the Designated Safeguarding Lead and approved by the Governing Body, and is reviewed sooner where statutory guidance changes.
- Parents may request a copy of this policy at any time; it is published on the school website.

ON REVIEW CYCLES

This policy is on an annual cycle. Keeping Children Safe in Education is reissued every year and has changed materially in each of the last four editions. Any online safety policy on a two- or three-year cycle will be out of date before its next review falls due.

Appendix A | Online safety incident response — decision route

This is the route for staff. It does not replace the Safeguarding and Child Protection Policy; it shows how an online concern enters it.

Stage	Who	Action
1. Notice	Any adult	Something concerns you: a disclosure, a monitoring alert, something seen on a screen, something reported by another child, something a parent tells you. You do not need to be sure.
2. Secure	Any adult	If a device is involved, secure it without examining it. Do not view, copy, forward or delete anything. Do not ask the child to show you.
3. Report	Any adult	Tell the Designated Safeguarding Lead the same day, in person. Record what you saw or were told, in the words used, as soon as you can.
4. Triage	DSL	Determine: safeguarding concern, behaviour matter, adult conduct matter, technical matter, or a combination. Record on [SYSTEM].
5. Immediate risk?	DSL	If a child is at immediate risk of harm: contact the police (999) and children's social care the same day. Do not wait for further information.
6. Illegal content?	DSL	Child sexual abuse imagery: report to the Internet Watch Foundation; do not view or copy. Terrorist or extremist content: report via GOV.UK and consider a Prevent referral. Concern about an adult contacting a child: report to CEOP. Other criminal content: police.
7. Adult at this school?	Headteacher	Allegations against an adult working at the school go to the Headteacher, who contacts the Local Authority Designated Officer. Concerns about the Headteacher go to the Chair of Governors. Do not discuss with the person concerned.
8. Harmful but not illegal	DSL	Report to the platform. Where the platform does not act, report to Report Harmful Content. Support the child and the family through the process.
9. Support	DSL	Put support in place for the child, and for any child who caused the harm. Consider whether an early help assessment is needed.
10. Learn	DSL and Computing Lead	Feed the incident theme into curriculum planning, staff briefing and, where relevant, the filtering and monitoring review.

Appendix B | Filtering and monitoring annual review record

Keeping Children Safe in Education 2026 requires the school to demonstrate that its filtering and monitoring effectiveness has been reviewed at least once every academic year. This record is that demonstration. It is completed, signed and presented to the Governing Body, and retained.

Academic year	
Date of review	
Review led by (senior leader, 5.3)	
Supported by (DSL)	
Supported by (IT provider)	
Date reported to Governing Body	

Section 1 | Provision

Question	Evidence / answer
What filtering system is in place, and what standard does it meet?	
What monitoring system is in place, and what type of monitoring is it (physical, live supervision, technology, or a combination)?	
Which device types are covered? (Desktops, laptops, Chromebooks, tablets, staff devices, personal devices on the guest network, visitor devices)	
Which locations are covered? (Classrooms, hall, library, outdoor areas, off-site use of school devices)	
What is NOT covered? State the gaps explicitly.	

Section 2 | Checks carried out

Check	Date	By whom	Result
Attempted access to blocked categories tested on each device type			
Attempted access tested in each location			
Monitoring alert generated deliberately and traced to the person who received it			
Time taken from alert to human review measured			
Out-of-hours alert handling tested			
Filtering tested for a pupil account, a staff account and a guest account separately			
Filtering tested against AI-generated and dynamically generated content			
Assistive technology and SEND access checked for over-blocking			

Section 3 | Effectiveness

Question	Answer
How many monitoring alerts were generated this year?	
How many were reviewed by a person?	
How many resulted in a safeguarding record?	
How many were false positives, and has the configuration been adjusted?	
Were there any filtering breaches? What happened and what changed?	
Does the provision address the risks in the school's Prevent risk assessment?	
Does the provision meet the DfE filtering and monitoring standards? Where it does not, what is the plan and by when?	

Section 4 | Actions and sign-off

Action	Owner	By when

Signed (senior leader responsible for filtering and monitoring)	
Signed (Headteacher)	
Signed (link governor for safeguarding and online safety)	
Date presented to Governing Body / minute reference	

Appendix C | Staff online safety self-audit

To be completed annually by all staff and volunteers and returned to the Designated Safeguarding Lead. Answers are used to plan training.

Name	
Role	
Date	

Question	Yes	No	Not sure
Do you know who the Designated Safeguarding Lead is and how to reach them today?			
Do you know who the senior leader responsible for filtering and monitoring is?			
Do you know exactly what to do if a pupil discloses an online concern to you?			
Do you know what to do — and what not to do — if you become aware of a nude or semi-nude image of a child?			
Do you know how to report a filtering breach, including one you caused accidentally?			
Have you read and signed the Staff ICT and AI Acceptable Use Agreement this academic year?			
Do you know which AI tools you are permitted to use, and what may never be entered into them?			
Do you know the school's position on mobile phones, including your own?			
Do you know what the school's monitoring software can and cannot detect?			
Have you read Part One of Keeping Children Safe in Education 2026 in full?			
Do you know the four Cs and could you give an example of each?			
Do you know how to report content that is harmful but not illegal?			

Which areas of online safety would you like further training on?

Appendix D | Local systems annex

This annex holds the detail that changes more often than the policy. It is updated whenever provision changes and is reviewed as part of the annual filtering and monitoring review. Updating this annex does not require the policy to be re-approved.

Item	Detail
Filtering provider and product	[ ]
Monitoring provider and product	[ ]
IT support provider	[ ]
Who receives monitoring alerts, and how	[ ]
Out-of-hours alert arrangement	[ ]
Safeguarding recording system	[ ]
Management information system	[ ]
Learning platform(s) used with pupils	[ ]
Pupil device types and where they are used	[ ]
Staff device types	[ ]
Guest network provision	[ ]
Approved AI tools for staff, and DPIA reference for each	[ ]
Position on pupil use of AI tools	[ ]
Mobile phone arrangement (storage, handover, responsibility)	[ ]
Data Protection Officer	[ ]
Senior leader responsible for filtering and monitoring	[ ]
Designated Safeguarding Lead	[ ]
Deputy Designated Safeguarding Leads	[ ]
Computing Lead	[ ]
Link governor for safeguarding and online safety	[ ]
Local Authority Designated Officer contact	[ ]
School website online safety page	[ ]
Date annex last updated	[ ]

Appendix E | Related policies and agreements

This policy is read alongside the following. Where this policy and another appear to conflict, the Safeguarding and Child Protection Policy takes precedence.

Document	Relationship to this policy
Safeguarding and Child Protection Policy	The governing document. All online safety concerns are handled under it.
Staff ICT and AI Acceptable Use Agreement	The signed agreement covering staff, governor, volunteer and visitor use of systems and AI. Signed annually. Not reproduced here.
Pupil Acceptable Use Agreement	Signed by pupils and countersigned by parents annually.
Behaviour Policy	The route for pupil misuse and for the mobile phone arrangement.
Anti-Bullying Policy	Read with section 12.
Data Protection Policy	Read with section 17.
Parent/Carer Code of Conduct	The route for parental online conduct.
Staff Code of Conduct	Professional conduct online, including social media and communication with pupils and parents.
Complaints Policy	The route for complaints about searches and about the operation of this policy.
Prevent risk assessment	Informs filtering decisions and is considered in the annual review.
RSHE and PSHE Policy	The taught content that sits alongside the computing curriculum.