



EDUCATION
EAST SUSSEX
TOGETHER FOR EXCELLENCE
AND INCLUSION



Incident Response Procedure

Alfriston Primary School

This policy was adopted on 30th September 2026

This policy is due for review on 1st September 2027



Contents

1. Purpose and scope	4
2. Statutory and guidance framework	4
3. Core response principles	4
4. Immediate response for all staff	5
5. Triage and decision-making	6
6. Safeguarding concerns involving children	6
7. Sharing nudes and semi-nudes, sexual imagery and AI-generated sexual content	7
8. Illegal or suspected illegal content	8
9. Cyberbullying, harassment, hate, threats and harmful communications	8
10. Grooming, exploitation, coercion, sexual extortion and criminal exploitation ..	9
11. Radicalisation and extremist content	9
12. AI-enabled harm, deepfakes, impersonation and smart devices	10
13. Filtering and monitoring alerts	10
14. Cyber security and personal data incidents	11
15. Concerns involving staff, volunteers or contractors	11
16. Mobile phones and confiscated devices	12
17. Parents, carers, other settings and external agencies	12
18. Recording, evidence and confidentiality	13
19. Supporting children and staff	13
20. Review, learning and assurance	14
Appendix A. Immediate staff response card	15

Incident Response Procedure

Appendix B. Incident triage matrix	16
Appendix C. Specialist response routes.....	17
Appendix D. Local contacts and escalation	18
Appendix E. Guidance and statutory reference framework	19

1. Purpose and scope

This procedure explains how the setting will recognise, report, triage, respond to, record and review online safety incidents and concerns. It applies whether the incident happens on site or off site, through setting-owned or personal technology, or through an online service, where it raises a safeguarding, behaviour, professional-conduct, cyber-security, privacy or welfare concern connected with the setting.

Online and offline harm are often connected. An incident should therefore be managed according to the underlying risk and impact, not simply according to the platform, device or technology involved.

The DSL has lead responsibility for safeguarding decisions. Technical staff, the DPO, senior leaders and external providers may support the response, but technology and technical investigation do not replace professional safeguarding judgement.

2. Statutory and guidance framework

KCSIE 2026 comes into force on 1 September 2026. It requires schools and colleges to treat online safety as part of safeguarding and to respond to concerns about abuse, exploitation, child-on-child harm and staff conduct through their child-protection arrangements.

This procedure also reflects the UK Council for Internet Safety's March 2024 advice on sharing nudes and semi-nudes, DfE Searching, Screening and Confiscation guidance where statutory school powers apply, DfE filtering and monitoring standards, DfE cyber-security standards and current DfE guidance on generative AI.

3. Core response principles

- Take every report seriously. Do not dismiss a concern because it happened online, outside setting hours or on a personal device.
- Safeguard first. Immediate safety and welfare take priority over discipline, reputation, evidence gathering or technical diagnosis.
- Report promptly. Staff must pass safeguarding concerns to the DSL or DDSL without delay.
- Do not investigate beyond your role. Frontline staff should establish only enough information to understand the immediate risk and make an appropriate referral.
- Do not blame or shame a child for online behaviour, including the creation or sharing of sexual imagery.

- Preserve useful information without creating further harm. Record what was reported, relevant usernames, URLs, dates/times and the nature of the concern where this can be done safely and lawfully.
- Do not unnecessarily view, copy, download, forward or retain harmful or illegal content.
- Use parallel routes where necessary. A single incident may require safeguarding, behaviour, cyber-security, data-protection, staff-conduct and police responses at the same time.
- Share information on a need-to-know basis and in line with safeguarding and data-protection requirements.
- Support all affected children, including those alleged to have caused harm, while maintaining appropriate safeguards and accountability.
- Review significant incidents so that lessons inform education, filtering and monitoring, technical controls, supervision and policy.

4. Immediate response for all staff

If an online safety concern comes to a member of staff's attention, they should:

Stage	Expectation
1. Make safe	Deal with any immediate risk of harm. If there is an emergency or immediate danger, follow emergency safeguarding arrangements and contact emergency services as required.
2. Listen	Allow the child or reporter to explain what has happened. Do not interrogate, ask leading questions or require unnecessary detail.
3. Reassure	Explain that they have done the right thing by reporting. Do not promise confidentiality; explain that information must be shared with people who can help.
4. Do not investigate	Do not search accounts, question multiple children, message alleged perpetrators, or browse device content unless this is specifically within your authorised role and the relevant procedure permits it.
5. Do not spread content	Do not forward, screenshot, download, copy or save harmful or sexual content. Follow the specialist rules in sections 7 and 8.
6. Report	Inform the DSL or safeguarding team promptly. Staff-conduct concerns must follow section 15.
7. Record	Make a factual record using the setting's safeguarding recording system, including what was said, what was observed, actions taken and who was informed.

5. Triage and decision-making

The DSL, or DDSL acting within delegated responsibilities, should assess the concern promptly. The purpose of triage is to identify immediate risk, the safeguarding pathway, who needs to know and whether external advice or referral is required.

Triage should consider:

- who is involved, their ages, vulnerabilities, SEND, communication needs and relationship to one another;
- whether there is immediate danger, threat, coercion, exploitation, self-harm or suicide risk, or risk of further distribution;
- whether an adult is involved in sexual or exploitative behaviour toward a child;
- whether the incident may constitute child-on-child abuse, sexual violence or sexual harassment;
- whether content is or may be illegal;
- whether the incident involves sexual imagery, deepfakes, nudification, synthetic sexual imagery or sexual extortion;
- whether the behaviour is repeated, targeted, discriminatory, threatening or part of wider bullying or abuse;
- whether accounts, devices, systems or personal data have been compromised;
- whether children at other settings are involved;
- whether parents/carers can safely be informed at this stage;
- whether police, children's social care, LADO, Prevent/Channel, the DPO/ICO, IWF, CEOP or another specialist agency should be involved; and
- what immediate support and protective measures are needed.

6. Safeguarding concerns involving children

Any online incident that may indicate abuse, neglect, exploitation, child-on-child abuse or another safeguarding concern must be handled under the Child Protection and Safeguarding Policy. The DSL should ensure the concern is recorded and, where thresholds are met, referred to the appropriate statutory agency.

- The fact that an incident occurred off site or on a personal device does not prevent the setting from taking safeguarding action.
- Behaviour and safeguarding responses may run in parallel. A behaviour sanction must not replace safeguarding assessment.
- Children who are alleged to have caused harm may themselves be vulnerable or at risk

and should be assessed and supported accordingly.

- Where there is a risk that online content will continue to circulate, the DSL should consider specialist reporting/removal routes and advice from police or other agencies.
- Where children from another setting are involved, DSL-to-DSL communication should be considered, subject to any police or safeguarding advice about preserving an investigation.

7. Sharing nudes and semi-nudes, sexual imagery and AI-generated sexual content

Incidents involving nude or semi-nude imagery of children must be managed using the current UKCIS advice. The same safeguarding approach should be applied to AI-generated or manipulated sexual imagery of children, including deepfake sexual imagery and nudification, while recognising that the exact legal classification may depend on the circumstances and should be referred for specialist advice where necessary.

7.1 What all staff must do

- Report the incident to the DSL or equivalent immediately.
- Do not view, copy, print, share, store or save the imagery, and do not ask a child to share, forward or download it.
- If imagery is shown unexpectedly or viewed accidentally, stop viewing as soon as possible, report this to the DSL and seek support if needed.
- Do not delete the imagery or ask the child to delete it before the DSL has assessed the incident and determined the appropriate next step.
- Do not question the child in detail about the imagery; obtain only the information necessary to establish immediate safety and make the referral.
- Do not blame or shame any child involved.

7.2 DSL response

- Follow the full UKCIS risk-assessment and safeguarding process.
- Consider the age and vulnerability of the children, consent or coercion, adult involvement, distribution, threats, exploitation, sexual extortion and whether the imagery has been shared beyond the original context.
- Viewing imagery should not be routine. In exceptional circumstances only, the DSL or DDSL may decide that viewing is necessary to safeguard a child, in line with the UKCIS guidance and professional judgement.

- Where an adult has shared sexual imagery of a child, treat this as child sexual abuse and seek urgent police/safeguarding advice.
- Decisions about deletion, retention or police evidence should follow the specialist guidance and any police direction rather than being improvised locally.
- Provide support to children and to any staff member who has been exposed to distressing imagery.

8. Illegal or suspected illegal content

If staff become aware of content that is or may be illegal, including suspected CSAM or unlawful terrorist material, they must avoid unnecessary viewing, copying or distribution and inform the DSL or appropriate senior lead immediately.

- Do not investigate the legality of content by searching for more examples.
- Do not forward suspected illegal content to colleagues, parents or external agencies by ordinary email or messaging.
- Record the source or URL where this can be done without opening or reproducing the content.
- Secure relevant devices or accounts where necessary without browsing their contents, pending advice.
- The DSL/DDSL should seek police or specialist advice where the criminal status or correct handling is unclear.
- Where appropriate, illegal online child sexual abuse material may be reported through the Internet Watch Foundation route; suspected criminal conduct affecting a child should still be considered through safeguarding and police routes.
- Where an immediate risk of serious harm exists, use emergency procedures.

9. Cyberbullying, harassment, hate, threats and harmful communications

Online bullying or harassment should be assessed for both safeguarding and behaviour implications. The response should reflect severity, repetition, power imbalance, discrimination, threats, sexual content, anonymity, scale of distribution and impact on the child.

- Preserve relevant messages or account details where this can be done safely, without encouraging further circulation of harmful or sexual material.

- Apply the Behaviour and Anti-bullying policies where appropriate, alongside safeguarding action.
- Threats of violence, stalking, targeted hate, doxxing (a form of harassment that involves publicly exposing someone's private information without their consent), sexual harassment or coercive behaviour may require police advice or referral.
- If harmful content is hosted publicly, the setting may consider platform reporting or specialist harmful-content reporting routes once this will not compromise police or safeguarding action.
- Support should focus on impact and safety, not solely on whether the behaviour occurred during setting hours.

10. Grooming, exploitation, coercion, sexual extortion and criminal exploitation

Online contact may form part of child sexual exploitation, criminal exploitation, grooming, coercive control, trafficking, county lines activity or other abuse. Any such concern must be escalated immediately to the DSL.

- Do not engage with the suspected offender from the child's account or attempt a sting or confrontation.
- Preserve account names, URLs, dates, times and reported communications where this can be done safely.
- Consider whether the child is under pressure to send money, sexual images, passwords, location information or other material.
- Sexual extortion should be treated as a safeguarding emergency where threats, blackmail, self-harm risk or rapid escalation are present.
- The DSL should consider police, children's social care and specialist child-exploitation routes according to risk.
- Parents/carers should normally be involved where it is safe and appropriate, but this decision must consider whether contact could increase risk or compromise an investigation.

11. Radicalisation and extremist content

Where online behaviour raises concern that a child is being drawn into terrorism, exposed to extremist grooming or otherwise at risk of radicalisation, staff must report the concern to the DSL and follow the setting's Prevent and safeguarding procedures.

- Do not confront or debate suspected extremist actors online.
- Assess the child's vulnerability, contact, intent, behaviour and wider safeguarding context.
- The DSL should use the local Prevent/Channel referral and police routes where appropriate.
- Illegal terrorist content should not be copied or circulated.

12. AI-enabled harm, deepfakes, impersonation and smart devices

AI can create new forms of harm or amplify existing safeguarding, fraud and abuse risks. The response should be based on the underlying harm rather than on whether AI was involved.

- Deepfakes, cloned voices, synthetic images or fake messages used to sexualise, humiliate, threaten, defraud or impersonate a person should be routed according to the safeguarding, behaviour, staff-conduct, cyber or police risk involved.
- AI-generated sexual imagery involving children must follow section 7 and the AI and Emerging Technology Procedure.
- Unsafe chatbot or AI-companion interactions should be assessed for sexual content, coercion, manipulation, self-harm, emotional dependency, grooming and vulnerability.
- If an AI service has received personal or safeguarding information without approval, the DPO should assess the privacy incident in parallel with any safeguarding response.
- Smart glasses, wearable cameras and AI-enabled wearables may create evidence, privacy or covert-recording issues. Do not access or search device contents outside authorised powers and procedures.
- Where AI-generated impersonation is used in a phishing or fraud attempt, follow cyber-security controls as well as safeguarding where a child is affected.

13. Filtering and monitoring alerts

Filtering and monitoring alerts are indicators that require professional triage; they are not conclusions about a child's intent or welfare. High-risk safeguarding alerts should be shared promptly through the agreed safeguarding route.

- The safeguarding team should assess the context, the child, the content category and any known vulnerabilities.
- IT or the monitoring provider should supply technical context without making the safeguarding decision.

- Routine reports and high-risk alerts should follow the distinct arrangements defined in the Filtering and Monitoring Standard.
- A lack of an alert does not mean that no safeguarding concern exists.
- Following a significant incident, the DSL and technical lead should review whether filtering or monitoring controls, categories, alert routing or supervision need to change.

14. Cyber security and personal data incidents

Some online safety incidents are also cyber-security or data-protection incidents. Safeguarding and technical response should run in parallel where necessary.

Incident	Response
Account compromise / phishing	Report to IT/cyber route immediately. Reset or contain access as directed. Inform DSL where a child or safeguarding system, storage area or emails have been affected.
Lost or stolen device	Report promptly. Consider remote containment, personal data exposure and safeguarding impact.
Data sent to wrong recipient / AI service	Notify DPO promptly. Assess containment, deletion, supplier contact and breach obligations. If the data shared has an impact on safeguarding, the DSL should also be informed.
Malware / ransomware / service disruption	Follow the cyber incident response plan and business continuity arrangements. Prioritise safeguarding and critical services.
Impersonation / cloned voice / fraudulent request	Treat as possible cybercrime or fraud; verify through an independent approved channel and escalate safeguarding where relevant.

15. Concerns involving staff, volunteers or contractors

Concerns about the online conduct of an adult working with children must be routed through the setting's staff-conduct, low-level concerns and allegations procedures as applicable. Staff must not investigate a colleague themselves.

- Concerns about a member of staff should be reported to the headteacher or other person named in the Child Protection and Safeguarding Policy.
- Concerns about the headteacher should follow the route specified in the Child

Protection and Safeguarding Policy, normally to the chair of Governors.

- The appropriate senior lead should consider whether the LADO must be consulted in line with KCSIE and local safeguarding procedures.
- If the concern involves possible criminal conduct, illegal imagery or immediate risk to a child, police and safeguarding agencies should be involved as appropriate.
- Relevant accounts or devices may need to be secured, but technical action must not compromise safeguarding, HR or police investigations.
- Personal social-media contact, inappropriate messaging, recording, impersonation or AI-generated sexual/harmful content involving pupils should be assessed against professional-boundary and safeguarding expectations.

16. Mobile phones and confiscated devices

Confiscation under the Mobile Phone and Personal Device Policy does not automatically authorise staff to browse a device. Searching for a device and examining content are separate matters.

- Where statutory school search powers apply, authorised staff must follow current DfE Searching, Screening and Confiscation guidance and the Behaviour Policy.
- If a device may contain safeguarding or criminal evidence, secure it appropriately and seek DSL/police advice before accessing content unless the legal guidance clearly authorises the specific action.
- For sharing nudes and semi-nudes incidents, the specialist rules in section 7 take precedence over routine behaviour handling.
- Do not require a child to unlock a device or show content simply to satisfy curiosity or establish a behaviour breach where safeguarding procedures require a different approach.
- Record who holds a confiscated device and how it is stored where the incident is significant.

17. Parents, carers, other settings and external agencies

Parents and carers should usually be informed of incidents involving their child where this is appropriate and safe. The DSL should decide timing and content where safeguarding or police considerations apply.

- Do not contact parents before consulting the DSL where this could place a child at greater risk, prejudice a police investigation or conflict with safeguarding advice.

- Where another setting's child is involved, use appropriate safeguarding channels to communicate with that setting, subject to agency advice.
- Public or media communication about a significant incident should be coordinated by authorised senior leaders and must not disclose safeguarding information.
- Where an incident extends beyond the setting, leaders should coordinate safeguarding, police, DPO, technical and communications responses so that actions do not conflict.
- External reporting/removal routes may include police, children's social care, LADO, Prevent/Channel, IWF, CEOP, the ICO or platform providers depending on the nature of the incident.

18. Recording, evidence and confidentiality

- Record factual information promptly: who reported the concern, when, what was said or observed, immediate risk, actions taken, referrals made and decisions reached.
- Record professional rationale for key decisions, including decisions not to refer externally.
- Avoid reproducing harmful content within safeguarding records where a description, URL or reference is sufficient.
- Do not store sexual imagery of children within routine safeguarding records.
- Technical logs, screenshots and other evidence should be handled proportionately and securely, with access limited to those who need it.
- Confidentiality is not secrecy: information should be shared when necessary to safeguard a child, but only with appropriate people and for a legitimate purpose.
- Retention should follow safeguarding, data-protection and records-management requirements.

19. Supporting children and staff

The response should include practical and emotional support, not only investigation or sanctions.

- Identify a trusted adult and support plan for affected children where appropriate.
- Consider changes to supervision, timetable, peer contact, device access or online accounts where needed for safety.
- Avoid arrangements that unnecessarily punish or isolate a child who has experienced harm.
- Provide age-appropriate information about reporting, blocking, account recovery and content-removal options where relevant.
- Consider SEND, communication needs, trauma, mental health, identity, protected

characteristics and other vulnerability factors.

- Offer appropriate support to staff who have been exposed to distressing sexual, violent or abusive material in the course of their role.

20. Review, learning and assurance

After significant incidents, leaders should review both the handling of the individual case and whether wider controls need to change.

- Review safeguarding practice, supervision and reporting routes.
- Review filtering and monitoring effectiveness, including alert routing and any technical limitations.
- Review cyber-security controls, account management and supplier response where relevant.
- Review AI-tool approval, smart-device or wearable controls where relevant.
- Consider curriculum, pupil education, staff training and parent/carers communication.
- Identify whether policies, acceptable-use agreements or local contacts need updating.
- Record lessons learned and track actions to completion.
- Provide appropriate assurance to governance without disclosing unnecessary personal or safeguarding information.

Appendix A. Immediate staff response card

If...	Do...
A child tells me something worrying happened online	Listen, reassure, do not investigate, report to DSL, make a factual record.
I see sexual imagery involving a child	Stop viewing. Do not copy, save, forward or delete. Report immediately to DSL.
A child wants to send me a sexual image as proof	Tell them not to send or forward it. Report to DSL.
I see suspected illegal content	Do not search for more or circulate it. Report to DSL/DDSL.
I receive a high-risk filtering/monitoring alert	Follow the agreed safeguarding triage route immediately.
A pupil reports blackmail / sexual extortion	Treat as urgent safeguarding; involve DSL immediately and consider self-harm/suicide risk.
A deepfake or AI-generated sexual image involves a child	Treat as a safeguarding sexual-imagery incident; follow section 7.
An account or device appears compromised	Report to IT/cyber route; involve DSL if safeguarding is affected.
A colleague's online conduct concerns me	Use the staff-conduct/allegations reporting route; do not investigate them yourself.
I am unsure what to do	Report to the DSL or DDSL. Do not delay because the technology or legal status is unclear.

Appendix B. Incident triage matrix

Type	Indicative priority	Primary route
Immediate danger / serious injury / credible imminent threat	Emergency	Protect life; use emergency safeguarding procedures; contact emergency services as required; inform DSL/DDSL.
Adult sexual contact or adult sharing sexual imagery of a child	Critical safeguarding	DSL; urgent police / children's social care advice; staff allegation route if adult is connected to setting.
Child sharing nudes/semi-nudes; deepfake sexual imagery; nudification	High safeguarding	DSL immediately; UKCIS process; do not view/copy/delete; assess coercion, exploitation and distribution.
Sexual extortion / blackmail / grooming	High safeguarding	DSL immediately; assess immediate emotional/self-harm risk; contact police/social care.
Serious threats, hate, stalking, doxxing or harassment	High / medium	DSL + behaviour; police advice where threat/crime threshold may be met.
Filtering/monitoring high-risk alert	High / variable	Safeguarding triage promptly; technical context from IT/provider.
Phishing, account compromise, malware, data loss	Cyber / data	IT/cyber + DPO; DSL where child/safeguarding impact.
Routine acceptable-use breach without safeguarding indicators	Behaviour / operational	Follow Behaviour/AUP process; escalate if new safeguarding information emerges.
Staff online conduct concern	Staff safeguarding / conduct	Headteacher or specified route; consider LADO/HR/police as required.

Appendix C. Specialist response routes

Concern	Specialist route	Key point
Sharing nudes / semi-nudes	UKCIS 2024 advice	DSL-led risk assessment; strict handling rules for imagery.
Suspected CSAM online	IWF / police as appropriate	Do not circulate; record URL/source safely; safeguarding response remains primary where a child is affected.
Online child exploitation / grooming	Police / children's social care / CEOP as appropriate	DSL determines referral route according to risk and local safeguarding procedures.
Radicalisation / terrorism risk	Local Prevent / Channel route; police where required	Follow Prevent and safeguarding procedures.
Cyber incident	Cyber Security and Account Management Standard	Parallel safeguarding route where children, safeguarding systems or pupil data are affected.
Personal data incident	DPO / Data Protection Lead; DSL depending on the data accessed/ potentially accessed	Assess breach, containment and notification duties; do not let data response delay safeguarding.
Staff allegation / low-level concern	KCSIE staff-conduct route / LADO as applicable	Do not investigate informally.
Harmful public content	Platform / specialist reporting route where appropriate	Preserve safeguarding/police investigation before takedown actions where necessary.

Appendix D. Local contacts and escalation

Role / service	Local details
DSL	Lindsey Hudson (Headteacher)
Deputy DSL	Tanya Fitzgerald (School Business Manager)
Headteacher	Lindsey Hudson (DSL)
Chair of Governors for concerns about headteacher	Simon Atkins & Yvette Aeberhard
Children's social care / safeguarding front door	Referrals into Early Help and Social Care Single Point of Access: 01323 464222 or Contacting the Single Point of Access (SPoA) East Sussex County Council
Out-of-hours children's social care	Emergency Duty Service (after hours, weekends and public holidays): 01273 335905
LADO	Consultation via the online portal here
Police non-emergency	101
Emergency services	999
Prevent / Channel	Report radicalisation or extremism
DPO	Roger Simmons
IT / cyber incident contact	ESCC Schools ICT
Filtering / monitoring provider escalation	ESCC Schools ICT
Local authority safeguarding advice	ESCC Safeguarding Team

Appendix E. Guidance and statutory reference framework

Source	Status	Relevance
<u>Keeping Children Safe in Education 2026</u>	Statutory guidance	Comes into force 1 September 2026.
<u>Sharing nudes and semi-nudes: advice for education settings working with children and young people (updated March 2024)</u>	UKCIS / government-published non-statutory advice	Specialist incident guidance for child/young-person nude and semi-nude imagery.
<u>Searching, Screening and Confiscation in Schools</u>	DfE guidance	Applies to specified school types; covers statutory search/confiscation powers.
<u>Filtering and Monitoring: Core Standard</u>	DfE digital and technology standard	Requires effective safeguarding-led monitoring/alert arrangements and review.
<u>Cyber Security: Core Standard / DfE cyber guidance</u>	DfE digital and technology standard / guidance	Supports cyber incident response, business continuity and technical containment.
<u>Generative AI in education and Safe use of generative AI in education</u>	DfE guidance / training	AI use must align with KCSIE, safeguarding, data, ethics and IP requirements.
<u>UK GDPR and Data Protection Act 2018, as amended</u>	Law	Relevant to incident records, monitoring logs, personal-data breaches and information sharing.
<u>Prevent Duty guidance</u> / local Channel arrangements	Statutory duty / guidance where applicable	Relevant to online radicalisation and terrorist-risk concerns.