



CROSFIELDS SCHOOL

Policy/Procedure Name:	Online Safety Policy
Policy Owner:	Director of Digital Strategy
Approved by:	Head Online Safety Governor
Approval Date:	September 2026
Date of next Review:	September 2027

Scope of the Online Safety Policy

This Online Safety Policy sets out how **Crosfields School (the School)** will safeguard members of our community online, in line with statutory guidance and best practice. The school is aware of the wider statutory requirements that informs this policy.

This policy applies to all members of the school community who access or use school digital systems, including staff, pupils, governors, volunteers, parents/carers, visitors and community users. It applies to use of school systems both on and off site, and to the use of personal devices on the school site (where permitted).

Where online safety concerns or incidents occur outside school and are known to the School, Crosfields School will respond in line with this policy and related procedures, including the School's Safeguarding and Child Protection Policy, Behaviour and Anti-Bullying policies. Where appropriate, parents/carers will be informed of incidents involving inappropriate online behaviour that take place out of school.

Policy development, monitoring and review

This policy has been developed by the Online Safety Group (part of the Crosfields' IT committee). Its membership and responsibilities are set out in the dedicated Online Safety Group section below.

Consultation with the wider School community has taken place through a range of formal and informal opportunities to ensure the policy is understood, workable and proportionate.

Schedule for approval, monitoring and review

Policy review cycle: reviewed annually, or sooner in response to significant technological developments, emerging risks, or incidents.

Escalation following serious incidents: The School Designated Safeguarding Lead will support in the escalation following any serious incidents. As part of this, the School may inform relevant external agencies as appropriate (e.g. Children's Services and/or the Police)"

Responsibilities

Online safety is a shared responsibility. All members of the Crosfields school community are expected to model safe, responsible behaviour, report concerns promptly and learn from incidents and good practice. The roles below clarify accountability.

Headteacher and senior leaders

Senior leaders set the culture and ensure that systems are effective. In line with [KCSIE](#), the DSL holds day-to-day lead responsibility.

Senior leaders will:

- Ensure the School meets its safeguarding duty of care, including online safety.
- Know and apply procedures for serious allegations involving staff (the Head plus at least one senior leader).
- Ensure that the DSL, IT provider/technical staff and relevant colleagues are trained and able to fulfil their roles.
- Ensure that all staff receive appropriate and timely online safety training which, amongst other things, includes an understanding of the expectations, applicable roles and responsibilities in relation to filtering and monitoring
- ensure that children are taught about how to keep themselves and others safe online, recognising that effective education will be tailored to the specific needs and vulnerabilities of individual children.
- Put in place appropriate oversight and support for internal monitoring activity. The DoDS will work with the DSL and IT provider on the annual review of the effectiveness of filtering and monitoring systems
- Ensure that regular online safety reports are received, and that emerging risks and themes are acted upon.

Governors

- Governors approve the Online Safety Policy on an annual basis and challenge its effectiveness as KCSIE requires them to:
- Ensure that all staff undergo safeguarding and child protection training on an annual basis (including online safety which, amongst other things, includes an understanding of the expectations, applicable roles and responsibilities in relation to filtering and monitoring – at induction and regularly updated)
- Ensure that children are taught about safeguarding, including in relation to online safety
- Review the DfE Filtering and Monitoring Standards and discuss with IT staff and service providers what more needs to be done to support the school in meeting this standard

The Governing Body will nominate a Online Safety Governor (OSG). The OSG will:

- Maintain an overview of information relating to online safety, filtering and monitoring, engaging with relevant school leaders and technical staff as appropriate.
- Support the School's compliance with statutory filtering and monitoring expectations.
- Undertake appropriate cyber security awareness training.

Designated Safeguarding Lead (DSL)

The Designated Safeguarding Lead (DSL) has lead responsibility for safeguarding and child protection, including online safety. The DSL will work with school leaders, IT staff, governors/trustees and relevant stakeholders to ensure effective safeguarding arrangements are in place, including appropriate filtering and monitoring systems, risk assessment, staff training and incident management. The DSL will ensure that concerns relating to online harm, cyberbullying, inappropriate content, AI-generated content, deepfakes, nude or semi-nude image incidents, and other technology-enabled safeguarding risks are identified, recorded, reported, responded to and managed in accordance with statutory guidance, local procedures and the school's safeguarding policies.

The DSL will:

- Lead safeguarding, including online safety, with clear responsibilities in their job description.
- Maintain up-to-date knowledge of online risks, filtering/monitoring and cyber security.
- Coordinate and record online safety concerns and incidents, escalating and referring in line with safeguarding procedures.
- Liaise with SLT, the Online Safety Governor, the IT provider and relevant external partners as required.
- Review anonymised incident patterns and filtering/monitoring information.
- Lead the annual review of the effectiveness of filtering and monitoring systems, in conjunction with the nominated SLT Lead and the IT provider
- Report regularly to SLT and drive continuous improvement across relevant policies and practice, using evidence (e.g. incident data, monitoring, self-review such as 360 safe).
- Ensure appropriate support for pupils with SEND.

The Online Safety Lead (DoDS) will support delivery of the Online Safety Policy; the DSL retains lead responsibility.

Director of Digital Strategy

The DoDS will:

- Lead the Online Safety Group and support the DSL day to day.

- Lead development and review of online safety documentation.
- Coordinate awareness, staff confidence and reporting readiness through appropriate training
- Work with curriculum leads to map, embed and evaluate online safety education.
- Liaise with IT and pastoral/support teams.
- Maintain current knowledge of risks across content, contact, conduct and commerce.

Curriculum Leads

Curriculum leads will work with the DSL/DDS to deliver a planned online safety programme through appropriate channels, e.g. Computing, PSHE/RSE, other curriculum areas, assemblies/pastoral provision and national initiatives including [Safer Internet Day](#).

Teaching and Support Staff

All staff are expected to uphold professional standards online and contribute to a strong safeguarding culture.

Staff will:

- Follow the Online Safety Policy, Safeguarding and Child Protection Policy, sign and comply with the Staff IT Acceptable Use Policy
- Maintain professional boundaries (including online/remote learning).
- Supervise learner use of technology and follow procedures for online safety issues
- Embed online safety where appropriate; teach research skills, copyright and plagiarism awareness.
- Challenge harmful online behaviour and report concerns promptly.
- Use only School-approved digital services and AI tools; protect data, apply UK GDPR, and verify AI outputs for accuracy/bias before use.
- Complete induction and annual training, with updates as needed; contribute to improvement by sharing learning and concerns.
-

IT service provider (EE)

The IT provider supports leaders and the DSL to meet DfE filtering, monitoring and technical standards. Where services are outsourced, the school remains accountable.

The IT provider will:

- Maintain secure infrastructure and managed user access.
- Implement, maintain and update filtering and monitoring; provide reports; act on alerts and concerns.
- Support procurement, risk identification, reviews and checks with SLT/DSL.
- Monitor systems for misuse and report concerns promptly to *the DSL*

- Follow the school's Online Safety and Technical Security policies and keep technical knowledge current.

Pupils

Pupils will:

- Follow the Pupils IT Acceptable Use Agreement and Online Safety Policy (including BYOD in years 10-11 only, no other personal devices, such as smartphones are permitted in school).
- Report concerns and know how to get help.
- Use technology responsibly, respecting others and their copyright and intellectual property.
- Use AI responsibly: protect original work, check accuracy and avoid plagiarism.
- Understand that out-of-school behaviour may be addressed where it affects the school community.

Parents and carers

Parents/carers are key partners in reinforcing safe online behaviour.

The School will:

- Publish the Online Safety Policy and share the learner Acceptable Use Agreement in pupil Teams and on the Crosfields School app
- Provide guidance on the responsible use of online technologies and seek permissions for digital services/images where required.
- Share updates through meetings, newsletters, online channels and campaigns.

Parents/carers will be encouraged to reinforce key messages and support safe use of personal devices (where permitted in the School).

Community users & visitors

Visitors to the school may request access to our guest Wi-Fi once they have signed it at reception using the Inventory system. Reception staff can provide a temporary guest password for them. Visitors are asked to refrain from smartphone use onsite, and not to take photos or videos.

Online Safety Group

The Online Safety Group (part of the Crosfields' IT committee) provides strategic oversight of online safety, monitors implementation and impact of the Online Safety Policy, and ensures online safety is embedded across safeguarding, curriculum and technical practice.

Membership

- Online Safety Governor
- Staff representatives including:

- Head
- DoDS
- Senior Deputy Head/DSL
- Deputy Head Academic
- Head/Deputy Head of Juniors
- DCO
- Curriculum Lead (Pre-prep)
- Pre-prep teacher
- Data & Systems manager
- Head of Computer Science (seniors)
- Senior IT Support Technician.

Core responsibilities

The group supports the DSL/DoDS to:

- Draft, review and monitor the Online Safety Policy and related documents.
- Oversee filtering and monitoring, including requests for change.
- Map and review online safety education for breadth, progression and relevance.
- Gather feedback from pupils, staff and parents/carers and turn this into improvement actions.
- Promote learner voice, peer support and awareness activity.

Governance and impact

- Operates to agreed Terms of Reference (membership, frequency, reporting lines), reviewed annually.
- Coordinates with Safeguarding, Behaviour, Curriculum, Digital Strategy and Pupil Voice as needed.
- Reports key themes, actions and impact to SLT and governors, and shares appropriate summaries with the wider community.

Acceptable use

Acceptable use is defined through the Online Safety Policy and Acceptable Use Agreements for staff and pupils Crosfields Acceptable Use Agreements (AUAs). These policies matter most when they are understood, reinforced and followed, not simply signed.

Reinforcement staff and learner induction/handbooks

- posters in areas where technology is used
- curriculum and awareness sessions
- communications with parents/carers
- School website
- peer support / learner-led activity

Acceptable/Unacceptable Actions

User actions		Acceptable	Acceptable at certain times	Acceptable for nominated	Unacceptable	Unacceptable & illegal
Users must not use online services (apps, games, sites) to create, share, download, upload, transfer or communicate material or comments that are:	Any illegal activity, for example: • Child sexual abuse imagery (CSAM)* • Child sexual abuse/exploitation and grooming • Terrorism-related content • Encouraging, promoting or assisting suicide/self-harm • Sexual image offences (including intimate image abuse/revenge porn and extreme pornography) • Incitement to, or threats of, violence • Hate crime • Public order offences (including harassment and stalking) • Drug-related offences • Weapons/firearms offences • Fraud and financial crime (including money laundering) • <i>Note: follow UKSIC and UKCIS guidance when responding to self-generated intimate images (SGII).</i>					X
Users must not attempt or support cybercrime (Computer Misuse Act)	• Misusing someone else's username/ID or password to access data, software or systems without authorisation • Gaining unauthorised access to school networks, data or					X

User actions		Acceptable	Acceptable at certain times	Acceptable for nominated	Unacceptable	Unacceptable & illegal
1990), including:	files (including bypassing security controls) • Creating, introducing or spreading malware (viruses, ransomware, harmful scripts) • Phishing, credential theft, or attempting to capture passwords or personal data • Revealing, copying or publishing confidential information (e.g., personal/financial data, databases, access codes) • Disabling, impairing or disrupting network/services (e.g., denial of service) • Using penetration-testing tools without explicit permission <i>Note: schools should decide whether incidents are dealt with internally or reported to police. Serious or repeat offences should be reported. The National Crime Agency provides routes to divert young people away from cybercrime and into positive pathways.</i>					
Unacceptable (not illegal) under school policies, for example:	Accessing inappropriate material/activities online in a school setting including pornography, gambling, drugs. (Informed by the school's filtering practices and/or AUAs)			X	X	
	Promoting discrimination, harassment or hateful content				X	

User actions		Acceptable	Acceptable at certain times	Acceptable for nominated	Unacceptable	Unacceptable & illegal
	Using school systems to run a private business or make unauthorised financial gain				X	
	Using tools/services to bypass filtering, monitoring or other safeguards (such as VPN/proxy, anonymisers, alternative DNS)				X	
	Infringing copyright or intellectual property (including via AI tools, stream ripping or unauthorised copying/sharing)				X	
	Unfair usage (downloading/uploading large files that hinders others in their use of the internet)			X	X	
	Sharing content that is offensive, undermines the school's ethos, breaches integrity, or brings the school into disrepute				X	

User Actions onsite	Staff and other adults				Pupils			
	Not allowed	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff oversight
Online gaming and in-game chat/voice (e.g. Roblox, Fortnite, Minecraft)	X				X			
Online shopping and digital commerce (including in-app purchases, marketplaces, subscriptions)			X		X			
Cloud storage and file sharing (e.g., Google Drive, OneDrive, Dropbox, WeTransfer; P2P/torrents)			X					X
Social media and user-generated platforms (e.g. TikTok, Instagram, Snapchat, X, Reddit) and other age-restricted services				X	X			
Messaging, chat and voice (e.g., WhatsApp, iMessage, Snapchat, Discord, Teams personal accounts)			X		X			

Streaming entertainment/media (video, music, podcasts) <i>e.g. Netflix, Disney+, Spotify</i>			X		X			
Video platforms and livestreaming (<i>e.g. YouTube, Twitch, TikTok LIVE, Instagram Live</i>)				X	X			
Personal mobile phones and smart devices on site (<i>phones, smartwatches, earbuds</i>).			X		X			
Taking photos/video/audio on devices		X						X
Other personal devices (<i>e.g., tablets, handheld consoles, VR headsets, wearables</i>)			X		X			
Personal email accounts on site or on the school network/Wi-Fi (<i>e.g., Gmail, Outlook.com</i>)			X		X			
School email used for personal communication (non-work/non-learning)			X				X	
Unapproved AI tools/services (<i>generative AI chatbots and image/video tools, AI companions, browser extensions</i>)	X				X			
Using AI to create, alter, generate, possess, share or distribute deepfake,	X				X			

manipulated, nude, semi-nude or sexually explicit images, audio or video of another person, or AI-generated content intended to harass, bully, humiliate, impersonate or cause harm								
---	--	--	--	--	--	--	--	--

The School recognises national findings, including the [Ofsted Review of Sexual Abuse in Schools and Colleges \(2021\)](#), which highlight that children may not always feel able to report. The school assumes that harmful online behaviours may be occurring, even where none have been disclosed, and responds by maintaining strong systems for reporting, analysing, and addressing concerns. KCSIE suggests that staff should have a professional curiosity and speak to the DSL (or a deputy) if they have concerns about a child

Reporting Concerns

The School will ensure that:

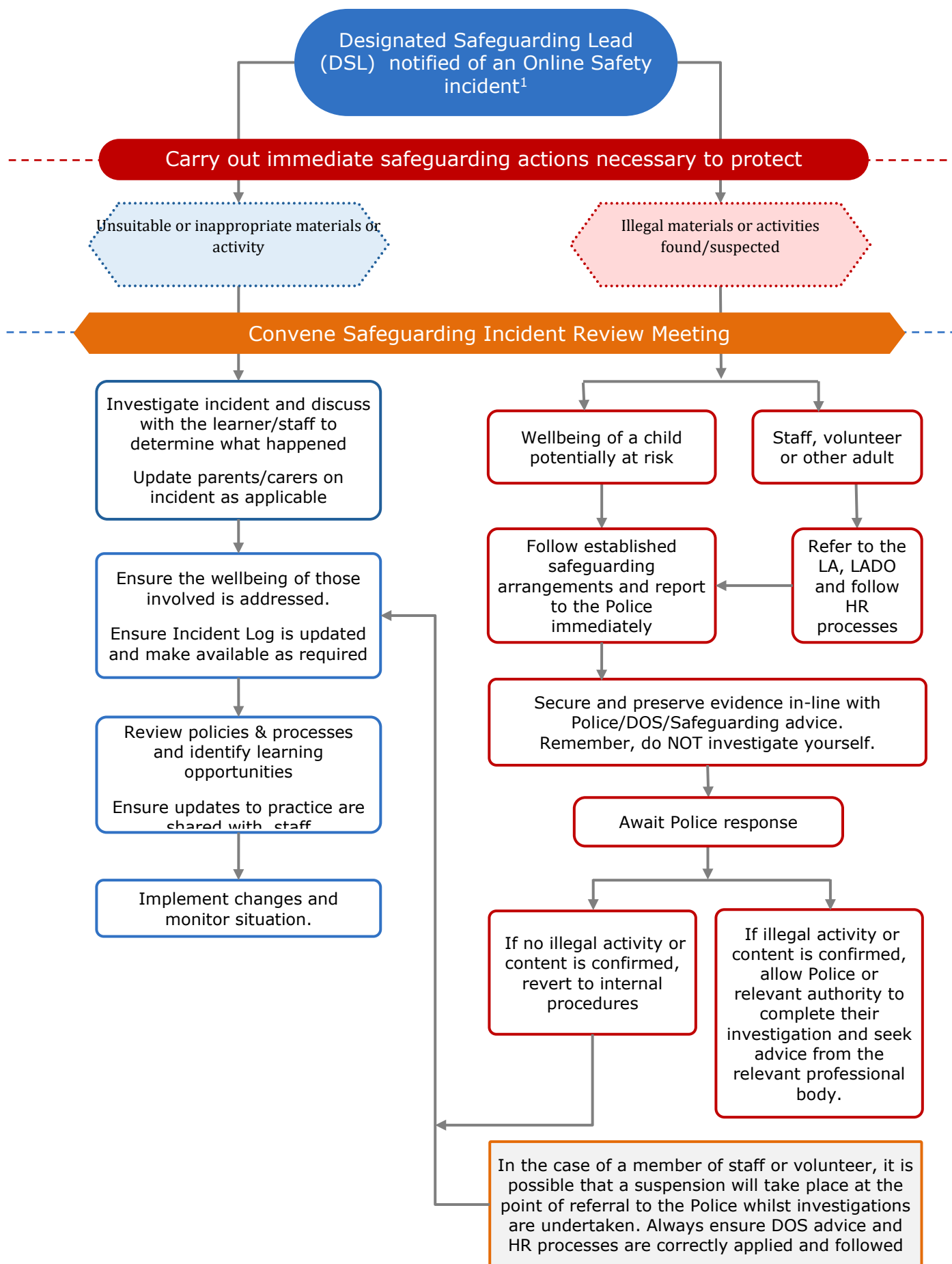
- Clear, accessible reporting routes are in place for all members of the School community, including pupils, staff, governors, parents/carers, and volunteers.
- Reporting processes are fully aligned with safeguarding procedures, including the child protection, whistleblowing, managing allegations and complaints policies.
- A variety of reporting options are available, such as speaking with the Designated Safeguarding Lead (DSL), online via "the worry button" (this is on the pupil intranet homepage), email contact, or in-person disclosures.
- Reporting routes are well publicised through induction, assemblies, posters, the School website, and other digital platforms.
- All users understand that any online safety concern must be reported, including those relating to harmful or illegal behaviour, sexual harassment, bullying, discrimination, grooming, or self-generated sexual imagery.

Responding to Concerns

The School will ensure that:

- Reports are acknowledged and responded to promptly, considering the safety and wellbeing of the person reporting.
- The DSL, DoDs, and senior leaders have the training and skills needed to recognise, assess, and manage online safety risks.
- Where a report indicates possible illegal activity or serious harm, it is escalated immediately through safeguarding procedures. Examples include (but are not limited to):
 - Child sexual abuse material (CSAM)
 - Non-consensual or self-generated images
 - Grooming, exploitation, or sexual harassment

- Terrorism or extremism
 - Hate crime, fraud, extortion, stalking
 - Cyber offences under the Computer Misuse Act
 - Sale of illegal substances or goods
- Where concerns do not involve suspected illegal activity, devices may be checked by IT staff, in the presence of an SLT member
- AI-supported monitoring systems, where used, are subject to human oversight to ensure contextual understanding.
- Users who report concerns receive reassurance, appropriate support, and feedback on the outcome.



Reporting Concerns

The School will ensure that:

- Clear, accessible reporting routes are in place for all members of the School community, including pupils, staff, governors, parents/carers, and volunteers.
- Reporting processes are fully aligned with safeguarding procedures, including the child protection, whistleblowing, managing allegations and complaints policies.
- A variety of reporting options are available, such as speaking with the Designated Safeguarding Lead (DSL), online via "the worry button" (this is on the pupil intranet homepage), email contact, or in-person disclosures.
- Reporting routes are well publicised through induction, assemblies, posters, the School website, and other digital platforms.
- All users understand that any online safety concern must be reported, including those relating to harmful or illegal behaviour, sexual harassment, bullying, discrimination, grooming, or self-generated sexual imagery.

Responding to Concerns

The School will ensure that:

- Reports are acknowledged and responded to promptly, considering the safety and wellbeing of the person reporting.
- The DSL, DoDs, and senior leaders have the training and skills needed to recognise, assess, and manage online safety risks.
- Where a report indicates possible illegal activity or serious harm, it is escalated immediately through safeguarding procedures. Examples include (but are not limited to):
 - Child sexual abuse material (CSAM)
 - Non-consensual or self-generated images
 - Grooming, exploitation, or sexual harassment
 - Terrorism or extremism
 - Hate crime, fraud, extortion, stalking
 - Cyber offences under the Computer Misuse Act
 - Sale of illegal substances or goods
- Where concerns do not involve suspected illegal activity, devices may be checked by IT staff, in the presence of an SLT member
- AI-supported monitoring systems, where used, are subject to human oversight to ensure contextual understanding.
- Users who report concerns receive reassurance, appropriate support, and feedback on the outcome.

Response to Incidents of Misuse

While serious incidents may occasionally occur, most cases are likely to involve inappropriate rather than illegal use of technology. The school will respond to all incidents promptly and proportionately, ensuring that appropriate action is taken in line with school policies and safeguarding procedures. Actions taken will reflect the nature and severity of the incident and, where appropriate, reinforce expectations for safe and responsible technology use.

Incidents of misuse by pupils will be addressed appropriately and proportionately, taking into account the nature and severity of the incident. Actions may include one or more of the following:

- Referral to the class teacher or tutor
- Referral to the Designated Safeguarding Lead (DSL) or Deputy Designated Safeguarding Lead (DDSL)
- Referral to the Senior Leadership Team (SLT)
- Referral to the Police and/or Social Services, where appropriate
- Referral to the school's IT service provider for investigation or technical intervention
- Informing parents/carers
- Issuing a warning and/or targeted intervention
- Temporary or permanent removal of device, network, internet, or system access rights
- Further sanctions in accordance with the school's Behaviour Policy

Incidents involving staff misuse of technology will be addressed appropriately and proportionately, depending on the nature, severity and circumstances of the incident. Actions may include one or more of the following:

- Referral to the member of staff's line manager
- Referral to the Senior Leadership Team (SLT) and/or Headteacher
- Referral to the Trust (MAT) or Local Authority (LA), where appropriate
- Referral to the Police and/or Local Authority Designated Officer (LADO)
- Referral to the School's IT Services Provider for investigation or technical support
- Issuing of a formal warning or management intervention
- Further disciplinary action in accordance with the School's Staff Disciplinary Policy and procedures

Use of Artificial Intelligence (AI)

Generative Artificial Intelligence (Gen AI) is evolving rapidly, with increasing applications across education. Crosfields School is committed to supporting the safe, ethical and responsible use of AI in teaching and learning, staff practice and school operations.

The School recognises that AI technologies can present safeguarding, data protection and information security risks. These are managed through existing policies, procedures and technical controls, supported by ongoing review and development as the technology evolves. Safeguarding remains central to our approach, and further guidance is provided in the School's Artificial Intelligence Policy.

Policy statements

The School will:

- Support appropriate use of AI to enhance learning and teaching, improve outcomes, streamline administration and reduce workload. Staff remain professionally responsible and accountable for any work supported by AI.
- Comply with relevant law and guidance, including Keeping Children Safe in Education 2026 (KCSIE) and UK GDPR.
- Provide training and guidance for staff and governors on the benefits, risks and safe use of AI, and identify further development needs.
- Teach about AI through the curriculum where appropriate, helping pupils understand how Gen AI works, its benefits and limitations, and its ethical and social impacts.

Safe use, data protection and security

The School will:

- Protect personal and sensitive data in line with the Data Protection Policy. Staff must not enter personally identifiable or sensitive information into AI tools. Where AI is used, staff should use anonymised data only.
- Require UK GDPR compliance. Staff must ensure any AI tool used meets data protection and security requirements before use.
- Approve tools and accounts. Only School-approved AI tools may be used for schoolwork, and staff should use school-provided AI accounts where available to support oversight and reduce risk.
- Safeguard sensitive information. Internal documents, strategic plans or other sensitive material must not be entered into third-party AI tools unless the tool and purpose have been explicitly approved.

Quality, fairness and integrity

The School will:

- Maintain human oversight. AI may support work but must not replace professional judgement—especially in decisions that affect people. AI outputs must be checked for accuracy before sharing or publishing.
- Promote transparency. Where AI has materially supported an output (e.g. documents, presentations, communications), staff should make this clear where appropriate.
- Address bias and discrimination. We recognise AI outputs may reflect bias. The school will use appropriate safeguards, review processes and procurement checks to prioritise fairness and safety.
- Protect copyright and intellectual property. The School will take steps to avoid copyright infringement and protect the intellectual property of staff and pupils, including ensuring pupils' work is not used to train AI systems without appropriate consent.

Reporting, monitoring and accountability

The School will:

- Require prompt reporting of AI-related concerns, including misuse, data incidents or inappropriate outputs, to the DoDs and DSL.
- Maintain an inventory of AI tools in use, with purposes and risks recorded, and carry out regular reviews of this
- Engage parents/carers with clear information about how AI is used in school

Use in assessment and feedback

AI tools may be used to support teachers with assessment processes (e.g. identifying areas for improvement and drafting feedback), and to support pupils in improving their work. Teachers remain responsible for outcomes and must ensure accuracy, fairness and appropriate use.

Misuse and disciplinary action

Improper use of AI—including breaches of this policy, data protection failures, misuse of sensitive information, or failure to follow agreed processes—may result in action under the school's Staff Disciplinary Policy. The school will not permit pupils to create AI-generated intimate images, deepfakes or synthetic content under any circumstances.

AI-Generated Imagery, Deepfakes and Nude/Semi-Nude Images

The School recognises that advances in artificial intelligence (AI) and image-generation technology have increased the risk of children being harmed through the creation, possession, sharing or distribution of digitally altered or wholly AI-generated images, videos and audio recordings.

For safeguarding purposes, the term **nudes and semi-nudes** includes images that have been:

- taken by the child;
- taken by another person;
- digitally altered or manipulated; or
- wholly generated using artificial intelligence, including so-called "deepfakes", "deep nudes" or "nudification" technologies.

The creation, possession, requesting, sharing or distribution of AI-generated or manipulated nude or semi-nude images involving children may constitute child-on-child abuse, online sexual harassment, bullying, exploitation and, in some circumstances, criminal behaviour. Such incidents will be treated as a safeguarding concern regardless of whether an original image existed.

Pupils must not use AI tools, apps, websites or other technologies to:

- create, edit, generate or manipulate images of any person without their consent;
- produce nude, semi-nude or sexually explicit images of children or adults;
- create deepfake images, videos or audio intended to humiliate, harass, bully, threaten, exploit or mislead others;
- impersonate pupils, staff or other individuals through AI-generated content; or
- share, store, request, forward or encourage the creation of such material.

Any concerns relating to AI-generated imagery, deepfakes or nudes and semi-nudes will be managed in accordance with the School's Safeguarding and Child Protection, Behaviour and Anti-Bullying Policies. The School will provide appropriate support for any child affected and will involve external agencies, including the police, children's social care or other relevant services, where necessary.

The school will educate pupils about the risks associated with AI-generated content, deepfakes and image-based abuse through its curriculum and safeguarding programme, promoting safe, responsible and ethical use of technology.

Education

Online Safety Education Programme

Online safety education is a core part of the School's safeguarding approach and sits alongside effective technical controls (including filtering and monitoring). In line with KCSIE, online safety is a running and interrelated theme reflected across relevant policies and the curriculum.

The School delivers a planned, progressive and inclusive programme of online safety education for all pupils, aligned to nationally recognised guidance and frameworks. Curriculum leads ensure learning is age-appropriate, builds on prior learning, is matched to need, and is taught through existing curriculum areas (including PSHE/RSE, Health Education, Computing and Citizenship), with assessment and clear intended outcomes.

The programme develops pupils' ability to:

- recognise and manage online risks, including harmful content, contact, conduct and commerce risks;
- understand consent, sexual harassment and sexual violence (including online), supported by safe opportunities for discussion;
- think critically about what they see online, including how to check reliability and accuracy and the role of AI-generated content;
- respect copyright and intellectual property, including when using online material and AI tools;
- understand and follow the learner acceptable use agreement, and act within moral and legal boundaries (including awareness of the [Computer Misuse Act 1990](#)).
- understand why online services use minimum-age requirements and how these may support safety, privacy and wellbeing
- make informed decisions about participation in social media, messaging, gaming and other online communities, including services they may not yet be permitted to use
- understand that legal or platform restrictions do not remove the need to learn about online relationships, harmful content, image sharing, scams, exploitation and digital wellbeing
- understand the School's mobile-phone requirements and the safeguarding, behaviour, learning and wellbeing reasons that underpin them.

Where internet use is planned, pupils are guided to appropriate resources and supported if unsuitable content is encountered. Where open searching is permitted, staff supervise and remain vigilant. Classroom Cloud software is installed on all school-managed devices, enabling searchable sites to be restricted as appropriate. Where legitimate curriculum research triggers a

Smoothwall alert, the activity must have a clear educational justification, appropriate approval where required, and an auditable rationale.

Pupil voice is actively used to strengthen the School's approach through feedback, learner representation, and opportunities such as digital leaders. Pupils are given appropriate opportunities to discuss changes affecting their digital lives and to express concerns about friendship, belonging, access, exclusion and wellbeing.

Staff

In line with [DfE Keeping Children Safe in Education \(KCSIE\) 2026](#), all staff and volunteers receive safeguarding and child protection training, including online safety, at induction and through regular updates (at least annually). Online safety training is integrated into the school's whole-school safeguarding approach, wider staff development and curriculum planning.

- A planned programme of online safety, data protection and cybersecurity training for all staff, regularly updated and reinforced. Staff training needs will be reviewed periodically to ensure provision remains relevant and effective.
- Staff understand the school's filtering and monitoring requirements, the responsibilities relevant to their role and how concerns or alerts must be reported
- Staff understand that filtering and monitoring supports - but does not replace - effective supervision, professional curiosity and safeguarding judgement
- Staff understand and consistently apply the School's mobile-phone requirements, including expectations for their own professional use of personal devices.
- Online safety and Cyber awareness training is provided for all new staff as part of induction, ensuring understanding of the Online Safety Policy and Acceptable Use Agreements, including classroom management, professional conduct, online reputation and modelling positive online behaviour.
- Regular updates for the Designated Safeguarding Lead and DoDS through external training and review of relevant guidance.
- Support for staff knowledge-building and consistent practice through structured professional learning resources.
- Regular review of this Online Safety Policy and updates through staff meetings, team briefings and/or INSET.
- Targeted advice, guidance and training from the DSL/DODS (or nominated staff) to individuals as required.

Governors

Governors should take part in online safety training and awareness activity. This is particularly important for governors serving on committees with responsibility for safeguarding, online safety, technology or health and safety.

Training and updates may be provided through (select/delete as appropriate):

- Participation in School training and information sessions (for example, staff briefings or parent events). This may include attendance at assemblies or lessons where appropriate.
- Regular update meetings with the DSL and/or DoDS to review key themes, incidents and current priorities.

Enhanced training will be provided for (at least) the Online Safety Governor. This will include:

- Basic cyber security awareness training.
- Training to understand the School's filtering and monitoring provision, enabling effective participation in required checks and reviews.

External Stakeholders

Families, the wider community and external agencies play a vital role in supporting the online safety education and wellbeing of pupils. The School recognises that parents and carers may have limited awareness of online risks so work to ensure parents are kept informed. The School may also draw on external agencies to supplement the School's safeguarding approach. The School therefore works actively to build strong partnerships, share key messages, and ensure that families and the wider community are equipped to help keep children safe online.

The following principles underpin the school's engagement with external stakeholders:

Working with Parents and Carers

The school will support parents and carers to understand online risks, build confidence, and reinforce safe online behaviours at home. This includes:

- Regular communication and awareness-raising about online safety issues, curriculum content, and reporting routes.
- Providing information through newsletters, the School website, learning platforms, and digital communication tools.
- Signposting parents and carers to trusted national resources (e.g. [UK Safer Internet Centre](#), [Internet Matters](#), [Childnet](#), [SWGfL](#)).

- Promoting and participating in key national events such as Safer Internet Day.
- Ensuring parents and carers understand acceptable use expectations and relevant school policies related to online safety.
- Clear communication about the School's Mobile Phone Policy and expectations, the reasons for the policy, authorised exceptions and the consequences of breaches
- Accurate, balanced and age-appropriate information about changes affecting social media and other online services
- Guidance and support for parents on managing and supporting their children's online experiences and how to report and manage issues.
- Guidance to help parents encourage their children to report online safeguarding concerns, regardless of any restrictions in place
- Mechanisms that evaluate the efficacy of School's strategy on mobile phones, online services and family engagement

Wider Community and Agencies

The School recognises the value of working with external organisations to strengthen local online safety awareness and provision. This includes providing and/or supporting family learning opportunities on digital technologies and safe online behaviours. The School may draw on the expertise of external agencies (e.g. UK Safer Internet Centre, CEOP, Local Safeguarding Partnerships, Prevent teams, police and health professionals), when appropriate.

Technology

Purpose

The School recognises that effective filtering, monitoring, technical security, cyber security and data protection are essential to safeguarding children and protecting the wider School community. These measures support safe and responsible use of technology while enabling effective teaching, learning and administration.

Filtering and Monitoring

The school uses the Smoothwall filtering and monitoring system to help protect users from illegal, inappropriate and harmful online content and activity, in line with statutory guidance. (e.g., [DfE Technical Standards](#), DfE [Generative AI: product safety standards](#); [KCSIE](#)) and best practice guidance (e.g., [UKSIC Appropriate Filtering and Monitoring](#)). The SLT and relevant staff have an awareness and understanding of the provisions in place and manage them effectively and know how to escalate concerns when identified.

The school ensures that:

- Filtering and monitoring arrangements are safeguarding-led, proportionate and regularly reviewed
- Filtering blocks illegal content and provides age-appropriate and role-appropriate access
- Monitoring supports the rapid identification of safeguarding concerns and enables timely intervention. Depending on severity, alerts to the DSLs and IT representative are triggered, prompting action.
- All School-owned devices are subject to filtering and monitoring onsite. Pupil devices are also monitored when used off-site, with internet access disabled over night for pupil well-being
- Staff and pupils understand that filtering and monitoring are in place, why they are needed, and how concerns are escalated
- Where the use of personal devices is allowed, users understand that their use may be filtered and monitored by the school.
- Where Generative AI products are used they must effectively and reliably prevent users from accessing harmful or inappropriate content and filtering mechanisms should be embedded within these products
- The technical limitations of the filtering system are understood, including whether the solution can monitor and filter real-time, dynamic, personalised or AI-generated content

Out of Hours Monitoring Alert Protocol

In the event of a serious **out of hours** monitoring alert, the monitoring service provider (Smoothwall) will make immediate telephone contact with members of school staff in the following order: The DSL, The Head, Head of Juniors, Head of Pre-Prep. The member of staff contacted will assess the risk and take appropriate action. If necessary, immediate contact will be made with the pupil's parents or any other relevant bodies in accordance with the School Safeguarding Policy. The incident will be followed up on the next school day.

Oversight and Review

- Senior leaders, the Designated Safeguarding Lead (DSL), technical staff and governors have clear roles and responsibilities
- Governors will review the DfE Filtering and Monitoring Standards and discuss with IT staff and service providers what needs to be done to support the school in meeting this standard.
- filtering and monitoring effectiveness is reviewed at least annually, and following significant changes or incidents.
- log reports provide actionable information for safeguarding decisions.
- no system is relied upon in isolation; reporting routes and professional judgement remain central

Technical Security

The School takes steps to ensure that its technical infrastructure is secure, reliable and well managed and meets its statutory requirements.

The school ensures that:

- access to systems and data is controlled through appropriate authentication and permissions
- devices, networks and systems are protected through secure configuration, patching and malware protection
- backups and recovery arrangements are in place to reduce the impact of system failure or attack
- incidents and weaknesses are reported, recorded and used to inform improvement
- responsibilities for technical security are clearly defined and supported by appropriate expertise
- systems are regularly reviewed and tested, meet statutory requirements and address emerging threats.

Cyber Security

The School recognises cyber security as a leadership and governance responsibility and takes steps to reduce the risk and impact of cyber incidents.

The school ensures that:

- a cyber security approach is in place to prevent, detect, respond to and recover from cyber threats
- senior leaders and governors understand cyber risks and their safeguarding implications receive appropriate assurance
- staff and pupils are educated/trained to recognise and report cyber security concerns
- business continuity and incident response arrangements are maintained and reviewed
- cyber security arrangements are kept under regular review and updated in line with emerging risks.

Data Protection

The School is committed to protecting personal data and complying with data protection legislation.

The School ensures that:

- personal data is processed lawfully, fairly and transparently
- a Data Protection Officer (DPO) is appointed, and appropriate governance arrangements are in place. The DPO role at Crosfields is undertaken by the Director of Compliance and Operations (DCO)
- all staff receive regular training to ensure they are aware of their responsibilities and can respond appropriately to data protection incidents.
- systems are in place to respond effectively to Freedom of Information and Subject Access Requests

- Data Protection Impact Assessments have been conducted on existing and planned use of software and systems.
- privacy notices explain how data is used and how individual rights can be exercised
- data is stored, shared and disposed of securely
- data breaches are reported and managed in line with legal requirements
- data protection is embedded across safeguarding, teaching, learning and administration
- where AI and Automated Decision-Making are in use, human oversight will be maintained for significant decisions, risk assessments will be conducted and the School will ensure automated systems are transparent and explainable.

Review

Arrangements for filtering, monitoring, technical/cyber security and data protection are reviewed regularly and updated to reflect:

- changes in technology
- emerging safeguarding risks
- national guidance and statutory expectations

Device Management

In line with Keeping Children Safe in Education (KCSIE), the School has clear expectations for the use of mobile phones, wearable technology and other digital devices to support safeguarding, learning and responsible behaviour.

The School ensures that:

- expectations for the use of School-owned and personal devices are clearly defined and communicated
- device use is consistent with safeguarding, behaviour, data protection and acceptable use policies
- appropriate technical and procedural controls are in place to support safe use
- staff and pupils have been trained/educated/informed and understand their responsibilities when using devices on school premises or systems
- education on the safe and responsible use of devices forms part of the School's online safety education
- Yondr Pouches are used in Seniors and pupils therefore do not have access to mobile phones or other personal smart devices throughout the school day, in accordance with the school's Behaviour and Mobile Phone policies (in line with the DfE statutory guidance)
- any exceptions are limited, clearly defined, authorised and managed appropriately, for example where required for medical, safeguarding, accessibility or SEND-related reasons
- Juniors and Seniors staff model the School's requirements and use personal devices only where authorised and professionally appropriate

- Within the Schools EYFS provision, personal mobile phones and devices are not accessible to children and must be kept securely stored throughout the school day. Staff must not use personal devices in the presence of children. Any use of digital technology in EYFS must be through school-approved devices and for legitimate educational, operational or safeguarding purposes only. procedures cover possession, storage, confiscation, searching and return of devices, in accordance with school policy and current national guidance.

Decisions about device use are informed by risk assessment and reviewed regularly.

Digital Content

The School recognises that multi-modal digital content (inc. AI) can enrich learning and communication when used responsibly. Its approach supports safeguarding requirements in particular, sexual imagery, consent, coercion, privacy and the sharing or manipulation of content.

The School ensures that:

- clear expectations are in place for the creation, use, storage and sharing of digital content
- consent, privacy and safeguarding considerations are applied consistently
- staff and pupils are trained/educated to understand their responsibilities when creating or sharing digital content
- personal data and images are handled securely and lawfully
- School-approved platforms and accounts are used where content includes personal or sensitive information
- staff and pupils understand that content may be copied, altered, republished or distributed beyond its intended audience, including through AI technologies
- AI-generated or AI-assisted content is reviewed for accuracy, legality, appropriateness, bias, transparency, copyright and safeguarding risk before use or publication
- policy and practice are reviewed in the light of emerging technologies and risks.

Public Online Communications

The School uses public online communications to inform, celebrate success and engage with the wider community, while managing associated risks. It supports KCSIE expectations around professional boundaries and staff conduct online, addresses reputational and safeguarding risk from public platforms while reinforcing parental engagement and transparency. The school understands that images posted online are at risk of AI manipulation and will follow guidance on this to protect our community

The school ensures that:

- public online communications are appropriate, accurate and well-managed
- public communications from or regarding the School are monitored and addressed where appropriate
- published content complies with safeguarding, data protection and statutory requirements
- guidance is followed to reduce the risk of illegal manipulation of publicly available images of staff and pupils,
- publishing public communications is restricted to authorised staff
- AI-assisted public communications are checked by an authorised person before publication and remain subject to human accountability. AI assisted content should be clearly labelled as such.
- online safety information is shared with parents, carers and the wider community
- clear processes exist for managing School online accounts
- staff understand expectations around professional conduct and online behaviour
- the school communicates confirmed changes to policy in line with best practice and Government guidance.

Review

Technology practice is reviewed regularly to reflect:

- changes in technology and online behaviour
- emerging safeguarding risks
- feedback from staff, pupils and parents
- national guidance and statutory expectations
- the School's progress towards meeting the DfE digital and technology standards
- the impact of mobile-phone arrangements and changes affecting children's access to online services.

•

Outcomes

The impact of the Online Safety Policy and practice is evaluated regularly using evidence such as online safety incident logs, behaviour and bullying records, and surveys of staff, pupils and parents/carers. Findings are reported to relevant groups and used to strengthen practice.

This process ensures that:

- Evidence from audits and reviews is discussed through balanced professional debate, alongside the impact of preventative work (education, awareness and training).
- Clear reporting routes are in place so patterns, themes and outcomes are shared regularly with senior leaders and governors.
- Parents/carers are informed of key patterns and learning through the School's online safety communication and awareness activity.
- Online safety and related policies and procedures, including the Data Protection Policy are updated in response to evidence and emerging risks.

- Learning and evidence of impact are shared, where appropriate, with other schools, agencies and local authorities to support a consistent local approach to online safety