BOURNEMOUTH SCHOOL FOR GIRLS

23 Online Safety Policy

For reference in this policy the current members of staff have the following roles at Bournemouth School for Girls:

Approved by	**FGB**	**Date: 8.7.26**	
Last reviewed by	Staff and Student Committee	Date: 9.6.26	Draft: May 2026
Next review due by	March 2027 or earlier if KCSIE/AI guidance changes	Policy owner	Online Safety Officer / DSL

Current named roles for reference: DSL Anna Collins (Deputy Headteacher); DDSLs Nicholas Weaver(Assistant Headteacher), Lisa Swan (Head of 6th Form) and Sarah Mantle (Head of House); Online Safety Officer Toby Osborne (Assistant Headteacher). The Deputy DSL may carry out roles assigned to the DSL within this policy.

Summary of key changes from previous policy

Area strengthened	What has changed
AI and online safety	AI is now treated as a core online safety issue, not only a homework or malpractice issue. The policy covers AI chatbots, deepfakes, voice cloning, nudification, synthetic media, AI-assisted grooming, scams, misinformation and image abuse.
Safety and data privacy first	The policy establishes a clear principle that no AI or online tool should be used with pupils unless safeguarding, data protection, filtering/monitoring and age-appropriateness have been considered.
Filtering and monitoring	Updated to reflect KCSIE 2025 and DfE filtering and monitoring standards, including annual review, roles, reporting failures, and application to AI tools.
KCSIE 2026 consultation readiness	Includes draft/proposed AI emphasis from the KCSIE 2026 consultation, without treating it as statutory until final publication.
Ofsted readiness	Links online safety to safeguarding culture, pupil voice, inclusion, curriculum, personal development and leadership/governance under the November 2025 Ofsted framework.

Image publication and AI abuse	Adds controls for pupil images and school publicity in light of increased deepfake and AI-CSAM/sextortion risks.
Acceptable use	Extends acceptable use expectations to AI tools, personal devices, unauthorised apps, data entry into AI tools and synthetic media creation.
Incident response	Adds a stronger triage model for online safety/AI incidents, including safeguarding, behaviour, IT/cyber, data protection and police/external agency routes.

Contents

- 1. Aims
- 2. Legislation and guidance
- 3. Core principles
- 4. The four categories of online risk
- 5. Roles and responsibilities
- 6. Filtering, monitoring, cyber security and technical controls
- 7. AI, synthetic media and online safety
- 8. Educating pupils about online safety
- 9. Educating parents/carers about online safety
- 10. Cyber-bullying and online child-on-child abuse
- 11. Searching, screening, confiscation and electronic devices
- 12. Acceptable use of the internet, digital systems and AI tools
- 13. Pupils using mobile, smart and wearable devices in school
- 14. Staff using work devices and online systems outside school
- 15. Use of pupil images, recordings and publicity
- 16. Responding to online safety incidents and misuse
- 17. Training and professional development
- 18. Monitoring, review and governance
- 19. Links with other policies
- Appendices

1. Aims

Bournemouth School for Girls aims to provide a safe, respectful and ambitious digital environment in which technology supports learning, communication, administration and personal development. Online safety is a core safeguarding responsibility and a whole-school responsibility.

The school will:

- have robust processes to safeguard pupils, staff, governors, volunteers and visitors online;
- identify and support pupils who may be at greater risk of online harm, including pupils with SEND, pupils known or previously known to children's social care, pupils with mental health needs, pupils who are socially isolated, and pupils who may face other barriers to safety or well-being;
- teach pupils to use technology safely, respectfully, responsibly, critically and lawfully;
- ensure that online safety, including AI-related online safety, is embedded in safeguarding, behaviour, curriculum, RSHE, ICT, homework, assessment, data protection and staff conduct;
- establish clear mechanisms to identify, report, intervene and escalate incidents;
- ensure that the school's use of digital and AI tools is purposeful, proportionate, safe, transparent and aligned with statutory duties;
- keep online safety practice under regular review because technology, online behaviour and associated harms change rapidly.

This policy should be read alongside the school's Artificial Intelligence Policy. The AI Policy provides the wider framework for the safe, ethical and educational use of AI; this Online Safety Policy explains how AI-related online risks are managed as part of safeguarding, digital conduct and technical controls.

2. Legislation and guidance

This policy is informed by current statutory and non-statutory guidance, including:

- Keeping Children Safe in Education 2025, including expectations around online safety, filtering and monitoring, cyber security, annual risk review and links to generative AI product safety expectations;
- the KCSIE 2026 consultation/draft proposals, which propose additional signposting to DfE generative AI policy and resources, with safeguarding, ethics and data protection implications. This draft material is used for readiness planning only and will be reviewed once final KCSIE 2026 is published;
- DfE guidance on generative AI in education, including the expectation that safety is the top priority and that pupil use of generative AI should only occur with appropriate safeguards, close supervision and tools with safety/filtering/monitoring features;
- DfE Generative AI: product safety expectations, including expectations around security, data protection, age-appropriate transparency, safeguarding alerts, prohibited content and administrator controls;
- DfE filtering and monitoring standards for schools and colleges;
- DfE cyber security standards for schools and colleges;
- DfE Teaching online safety in schools;
- DfE guidance on relationships education, relationships and sex education and health education;
- DfE Searching, screening and confiscation guidance;
- UKCIS guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people;
- Prevent duty guidance and guidance on protecting children from radicalisation;
- Ofsted Education Inspection Framework and State-funded School Inspection Toolkit for use from November 2025, including safeguarding, inclusion, personal development and leadership/governance expectations;
- Data Protection Act 2018, UK GDPR, Equality Act 2010, Education Act 1996, Education and Inspections Act 2006, Education Act 2011, Online Safety Act 2023 and relevant cyber-crime legislation.

3. Core principles

Principle	Policy position
Safety first	Digital tools, online platforms and AI systems must not compromise safeguarding, pupil welfare, data protection, equality, assessment integrity or professional standards.
Privacy first	Personal, sensitive, confidential or safeguarding information must not be entered into unapproved online or AI tools. Pupil images, recordings and work must be handled carefully.
Human accountability	Technology may support decision-making, but safeguarding, pastoral, assessment and disciplinary decisions remain human professional decisions.
Education, not avoidance	Pupils need to learn how to use technology critically, safely and ethically, including understanding AI, misinformation, manipulation, privacy and reporting routes.
Proportionate innovation	AI and digital tools may reduce workload and enrich learning when selected carefully, risk assessed, age appropriate and implemented with oversight.
Inclusion and accessibility	Online safety education and reporting routes must be accessible to all pupils, including pupils with SEND and those who may find disclosure difficult.
Whole-school culture	Online safety is not just an IT issue. It is part of safeguarding, behaviour, curriculum, pastoral care, governance and staff professional conduct.

[4. The four categories of online risk

The school's approach to online safety continues to be based on the four areas of risk described in KCSIE. These are now interpreted in light of rapidly developing AI tools, social media, gaming platforms, messaging apps, image-sharing platforms and online financial risks.

Risk category	Examples of risk, including AI-related risks
Content	Exposure to illegal, inappropriate or harmful content, including pornography, self-harm, suicide, misogyny, racism, antisemitism, extremism, radicalisation, conspiracy theories, misinformation, disinformation, fake news, harmful AI-generated content, synthetic images/videos, and AI-generated sexual or violent material.
Contact	Harmful online interaction with others, including grooming, exploitation, peer pressure, coercion, scams, impersonation, adults posing as children, AI-assisted grooming scripts, fake profiles, chatbots that encourage unsafe behaviour, and contact linked to criminal, sexual, financial or extremist exploitation.
Conduct	Online behaviour that causes harm, including cyber-bullying, harassment, misogynistic abuse, sharing nudes or semi-nudes, creating or sharing deepfakes, nudification images, voice cloning, impersonation, doxxing, recording without consent, sextortion, and using AI to humiliate, threaten, deceive or blackmail.
Commerce	Online gambling, inappropriate advertising, loot boxes, scams, phishing, financial fraud, fake school communications, AI-generated fraudulent emails, malware links, subscription traps and commercial exploitation of children's data or attention.

5. Roles and responsibilities

5.1 The governing board

The governing board has overall responsibility for monitoring this policy and holding the Headteacher to account for its implementation. The governing board will ensure that online safety is a running and interrelated theme across safeguarding, curriculum, behaviour, staff conduct, data protection, ICT, filtering and monitoring, AI governance and school improvement.

- ensure that all staff receive online safety training as part of safeguarding training and understand their responsibilities for filtering and monitoring;
- ensure that the school has appropriate filtering and monitoring systems on school devices and networks and reviews their effectiveness at least annually;
- ensure that the DfE filtering and monitoring standards, cyber security standards and generative AI product safety expectations are considered when reviewing systems and procurement;
- ensure that online safety, including AI risk, is included in governor safeguarding oversight and challenge;

- ensure that pupils are taught how to keep themselves and others safe online, including in relation to AI-generated content and synthetic media;
- ensure teaching about safeguarding and online safety is adapted for vulnerable pupils and pupils with SEND where necessary;
- ensure leaders can evidence the rationale, risk assessment and impact of any school-approved AI or digital tool.

The governor who oversees online safety is Mr Adam Mills. Governors must agree and adhere to the acceptable use agreement for staff, governors, volunteers and visitors.

5.2 The Headteacher

The Headteacher is responsible for ensuring that this policy is understood and implemented consistently. The Headteacher will ensure that online safety is integrated into safeguarding culture, curriculum planning, behaviour systems, staff conduct, parental communication, data protection and the school's AI governance arrangements.

5.3 Designated Safeguarding Lead and Online Safety Officer

The DSL has overall responsibility for online safety as part of safeguarding. At BSG, the Online Safety Officer supports and shares this role. The responsibilities include:

- supporting the Headteacher to ensure this policy is implemented consistently;
- taking the lead on understanding filtering and monitoring systems and processes on school devices and networks;
- working with the ICT Manager to ensure technical systems are effective, proportionate and reviewed;
- ensuring online safety incidents, including AI-related incidents, are recorded, triaged and escalated appropriately;
- ensuring concerns involving nudes, semi-nudes, sexual images, deepfakes, nudification, AI-CSAM, sextortion, grooming or exploitation are managed in line with safeguarding guidance and, where necessary, external agencies;
- ensuring concerns about radicalisation, extremist material or online grooming are referred through the appropriate Prevent or safeguarding routes;
- supporting staff to understand emerging risks, including AI-generated harm, misinformation, scams and online coercion;
- liaising with parents/carers, agencies, police, social care, IT support and external providers as necessary;
- providing regular reports to the Headteacher and governing board, including themes, trends and actions from online safety logs;
- leading or supporting the annual online safety risk assessment and review.

The designated Online Safety Officer is currently Toby Osborne (Assistant Headteacher).

5.4 ICT Manager / IT support

- maintain appropriate security protection procedures, including filtering and monitoring systems on school devices and networks;
- review and update security, filtering and monitoring systems at least annually and when significant risks, incidents or system changes occur;
- block harmful and inappropriate content without unreasonably restricting teaching and learning;
- support the DSL and Online Safety Officer in investigating filtering/monitoring failures or technology-related incidents;
- ensure systems are protected against malware, phishing, unauthorised access and cyber-attacks;
- support due diligence for approved digital and AI tools, including data protection, access control, age suitability and monitoring features;
- maintain clear procedures for staff to request access to blocked sites for legitimate educational purposes;

- report significant cyber incidents, data breaches or safeguarding-relevant monitoring alerts in line with school procedures.

5.5 All staff, volunteers, contractors and agency staff

- maintain an understanding of this policy and the linked AI Policy;
- model safe, professional and lawful technology use;
- follow acceptable use expectations for school systems, personal devices used for school work, online platforms and AI tools;
- report online safety concerns, filtering/monitoring failures and AI-related safeguarding concerns promptly to the DSL, Online Safety Officer or IT Manager as appropriate;
- use only approved or risk-assessed systems when working with pupils or school data;
- not upload pupil personal data, pupil work, images, safeguarding information or confidential school information into unapproved AI tools;
- provide pupils with safe, specific URLs or resources for online learning rather than asking pupils to search freely where this may increase risk;
- maintain an attitude of “it could happen here” in relation to online abuse, child-on-child abuse, sexual harassment, exploitation and AI-enabled harm.

5.6 Parents/carers

- support the school’s online safety expectations, including acceptable use and mobile phone rules;
- raise concerns with the school where they become aware of online harm, AI-generated abuse, cyber-bullying, image sharing, grooming, sextortion, scams or inappropriate contact;
- support pupils to use digital technology and AI tools safely, lawfully and age-appropriately outside school;
- engage with school communications and parent guidance on online safety and AI risks.

6. Filtering, monitoring, cyber security and technical controls

The school will maintain filtering and monitoring systems that are appropriate to its context and pupils’ needs. These systems will be designed to prevent access to harmful and inappropriate content while enabling effective teaching and learning.

The school will:

- identify and assign roles and responsibilities for filtering and monitoring;
- review filtering and monitoring provision at least annually and after significant incidents or system changes;
- block harmful and inappropriate content, including child sexual abuse material, terrorist content, pornography, extreme violence, self-harm/suicide content and other harmful material;
- maintain effective monitoring strategies that meet safeguarding needs;
- ensure staff know how to report concerns about over-blocking, under-blocking, monitoring failures or unsafe access;
- ensure that requests to bypass filtering for legitimate educational reasons are authorised and recorded appropriately;
- consider how filtering and monitoring apply to AI tools, including generative AI chatbots, image generators, translation tools, browser-integrated AI, search-integrated AI and embedded AI features within common applications;
- review cyber security arrangements periodically, recognising that generative AI can increase the sophistication of phishing, impersonation, malware and social engineering attacks.

Generative AI tools introduced for staff or pupil use must be considered against the DfE generative AI product safety expectations, including security, privacy, data handling, administrator controls, reporting, safeguarding alerts, age suitability, harmful content prevention and compatibility with filtering and monitoring standards.

7. AI, synthetic media and online safety

AI is now part of online safety. Generative AI tools can create text, images, audio, code, video, summaries, fake communications, synthetic voices, realistic photographs and manipulated media. These tools have potential benefits for workload efficiency, accessibility, teaching preparation, learning support and creativity, but they also create significant safeguarding, privacy, assessment, equality and mental health risks.

7.1 Safe and approved use

- Pupils may only use generative AI in school where a member of staff has explicitly permitted it for a clear educational purpose and appropriate safeguards are in place.
- Staff must not direct pupils to use open-access AI tools that are not age-appropriate, approved, supervised or risk assessed.
- Staff must not enter personal, sensitive, confidential, safeguarding or identifiable pupil information into unapproved AI tools.
- Pupil-facing AI tools must be age appropriate, supervised, aligned with filtering/monitoring expectations and risk assessed before use.
- Teacher-facing AI tools may support workload and development, but the member of staff remains responsible for checking accuracy, bias, appropriateness and compliance with school policy.
- AI tools must not be used to make automated safeguarding, pastoral, behaviour, SEND, admissions, assessment, exclusion or other high-stakes decisions about pupils.

7.2 AI-related harms and prohibited conduct

The school will treat the following as serious online safety concerns and, where appropriate, safeguarding, behaviour, data protection, police or external-agency matters:

- creating, requesting, possessing, sharing or threatening to share nude, semi-nude, sexualised or intimate images of pupils, including AI-generated or AI-manipulated images;
- using nudification apps, deepfake tools, face-swap tools or image generators to create sexualised or humiliating content involving pupils, staff or others;
- using AI to impersonate pupils, staff, parents, the school or external agencies;
- creating fake emails, letters, screenshots, voice notes, images, videos or social media posts that mislead, harass, bully, extort or damage reputation;
- using AI to support grooming, coercion, blackmail, sexual exploitation, criminal exploitation, radicalisation, fraud or cyber-bullying;
- creating or sharing misinformation, disinformation, hateful content, extremist material or harmful advice using AI tools;
- using AI to bypass school filtering, monitoring, security controls or assessment rules;
- uploading other people's images, voice, work, personal data or confidential information into AI tools without permission and a lawful basis.

7.3 Deepfakes, nudification and AI-generated sexual imagery

The school recognises the growing risk of AI-generated sexual imagery, deepfake pornography, nudification tools and sextortion. Such material can cause significant harm even where the image is artificially generated. Where the material involves a child or appears to involve a child, staff must treat the incident as a safeguarding concern and follow the DSL route immediately.

Staff must not view, copy, print, share or forward suspected indecent images of children, including AI-generated or AI-manipulated images. Devices or accounts should be secured and the DSL should decide next steps in line with UKCIS and DfE guidance.

7.4 AI and misinformation

Online safety education will teach pupils that AI systems can produce confident but false information, fabricated sources, biased outputs and persuasive misinformation. Pupils will be supported to evaluate online information, triangulate sources, identify manipulation and understand when to seek adult help.

8. Educating pupils about online safety

Pupils will be taught about online safety through the curriculum, including computing, RSHE/PSHE, tutor time, assemblies, subject teaching, pastoral support and targeted interventions. Teaching will be adapted where necessary for vulnerable pupils, victims of abuse and pupils with SEND.

Area of learning	Pupils will learn about
Digital conduct	Respectful communication, consent, kindness, digital footprints, online reputation, cyber-bullying, harassment, misogyny, racism, hate, and the impact of sharing content.
Online relationships	Grooming, coercion, exploitation, impersonation, fake profiles, pressure to share images, sextortion, and how to report concerns.
Privacy and data	Personal data, passwords, account security, location sharing, image consent, privacy settings, scams, phishing and how data is collected and used online.
Harmful content	Pornography, self-harm, suicide, extremist material, conspiracy theories, misinformation, disinformation, manipulated media and how to seek support.
AI literacy	How generative AI works at a basic level, its benefits and limits, hallucinations, bias, source checking, academic integrity, ethical use and the risks of deepfakes or AI-generated content.
Reporting and support	How to report concerns in school and externally, including where a pupil has made a mistake or is worried about something they have seen, sent or received.

Year 10 students will continue to receive an online safety talk alongside PSHE/SE lessons, with complementary parent/carer engagement where appropriate. Year 11 students will continue to receive support through “learning curve” or study lessons on healthy study habits, safe online working and responsible technology use.

9. Educating parents/carers about online safety

The school will raise parent/carer awareness of online safety through communications, the website, information evenings, targeted guidance and sharing of relevant resources. Parent/carer engagement will include AI-related risks where appropriate.

- the systems the school uses to filter and monitor online use;
- the sites, apps or platforms pupils are expected to use for learning;
- the school’s expectations around mobile phones, acceptable use and AI use;
- risks such as cyber-bullying, image sharing, deepfakes, nudification apps, sextortion, grooming, scams, misinformation and unsafe AI tools;
- how parents/carers can report concerns to school and seek help from external agencies.

Teachers must continue to provide specific URLs for required online resources used for homework or self-study and must consider whether the sites are safe, age appropriate and educationally relevant.

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

Cyber-bullying takes place online, including through social media, messaging apps, gaming platforms, collaborative documents, image-sharing platforms, email, AI tools or other digital environments. It includes repetitive or intentional harm, but a single serious incident may also require safeguarding or behaviour action.

Online child-on-child abuse may include abusive messages, threats, harassment, misogynistic content, racism, homophobia, transphobia, sharing of nudes or semi-nudes, AI-generated sexual imagery, deepfakes, coercion, humiliation, impersonation, doxxing, exclusion from online groups, and the sharing of abusive images or pornography.

The school will respond in line with the Behaviour Policy, Anti-Bullying Policy, Child Protection and Safeguarding Policy and this policy. Where illegal, inappropriate or harmful material has been created or shared, the school will seek to contain the incident, safeguard those affected and involve external agencies where necessary.

11. Searching, screening, confiscation and electronic devices

The Headteacher and authorised staff may search, screen and confiscate electronic devices in line with DfE guidance and the school's behaviour/searches policy where they have reasonable grounds to suspect that a device poses a risk, contains evidence relating to an offence, is a banned item, or has been or could be used to cause harm or disrupt the safe environment of the school.

If a staff member suspects a device contains an indecent image of a child, nude/semi-nude image, AI-generated sexual image, deepfake, nudification image or other image that may place a person at risk, they must not view the image and must report immediately to the DSL. The DSL will decide next steps in line with DfE and UKCIS guidance.

If material may constitute evidence of an offence, staff must not delete it. The device should be secured and advice sought from the DSL and, where appropriate, police or external safeguarding partners.

12. Acceptable use of the internet, digital systems and AI tools

Use of the school's internet, ICT systems, online platforms and AI tools must be for educational purposes or for the purpose of fulfilling an individual's school role. All users must follow the relevant acceptable use agreement.

- Pupils must not access, create, share or attempt to access illegal, inappropriate or harmful content.
- Pupils must not use AI tools in school unless explicitly permitted and supervised by staff.
- Pupils must not use AI to bully, harass, impersonate, cheat, generate harmful content, create fake evidence, bypass filtering or create sexualised/manipulated images.
- Staff must use school systems responsibly and must not use unapproved tools in ways that risk pupil safety, data protection, confidentiality, assessment integrity or professional standards.
- The school may monitor use of school systems, devices and networks in line with safeguarding, data protection and acceptable use expectations.

13. Pupils using mobile, smart and wearable devices in school

Currently, student BYOD policy is being reviewed in line with the Government Agenda regarding banning of smartphones in schools. There are current consultations and SLT level discussions about rolling out new controls and rules to decrease risk of poor behaviours by students using such devices and ensure a more controlled environment in terms of misuse whilst on school site. This subsection will need updating to reflect the new policies coming into force.

Where a device is used for an authorised educational purpose, the member of staff must ensure that

, photograph, livestream, share, upload or process images, audio or video of others without permission.

14. Staff using work devices and online systems outside school

Staff must take appropriate steps to ensure work devices and accounts remain secure, including strong passwords, locking devices when unattended, keeping operating systems updated, using anti-virus/anti-malware protection where applicable on personal devices if used, avoiding shared use by family or friends, and reporting security concerns promptly to the IT Manager.

Staff must not use school devices, school accounts, personal devices or personal accounts to upload pupil data, pupil work, pupil images, safeguarding information or confidential school information into unapproved AI tools. AI-supported work must comply with the school AI Policy, Data Protection Policy and Staff Code of Conduct.

15. Use of pupil images, recordings and publicity

The school recognises that publicly available pupil images can now be misused through AI-enabled scraping, face-swapping, nudification, impersonation and sextortion. The school will continue to celebrate pupil achievement while applying proportionate safeguards.

- Pupil images and recordings must only be taken, stored and shared in line with parental permissions, school procedures and data protection expectations.
- Staff must consider whether images used publicly are necessary, proportionate and safe, particularly where pupils are identifiable by name, uniform, activity, location or metadata.
- The school will consider safer publication approaches where appropriate, such as group images, non-close-up images, reduced metadata, avoiding full names, restricting downloadability, using privacy settings, or using non-identifiable images.
- Images or recordings must not be uploaded into AI tools unless this has been specifically approved through risk assessment, data protection consideration and a clear educational purpose.
- Any concern that a pupil image has been manipulated, sexualised, deepfaked or used for blackmail must be reported immediately to the DSL.

16. Responding to online safety incidents and misuse

The school will respond to online safety incidents proportionately, with safeguarding as the first consideration. Incidents may require behaviour action, pastoral support, safeguarding referral, IT/cyber response, data protection action, parental communication and/or police involvement.

Incident type	Initial response route
Safeguarding risk to a pupil	Report immediately to the DSL/Deputy DSL. Record on the safeguarding system. Consider external referral where threshold is met.
Nudes, semi-nudes, deepfakes, nudification, AI sexual imagery or sextortion	Do not view, copy or share. Secure device/account if needed. Report immediately to DSL. Follow UKCIS/DfE guidance and consider police/social care advice.
Cyber-bullying, harassment or online child-on-child abuse	Follow Behaviour/Anti-Bullying and safeguarding procedures. Support victim, address perpetrator behaviour, consider wider peer context.
Filtering/monitoring failure	Report to IT Manager and Online Safety Officer/DSL. Record issue, assess risk and remedy promptly.
Data breach or unauthorised data sharing	Report to Data Protection Officer. Follow data breach procedure and consider ICO reporting threshold.
Cyber security incident, phishing or malware	Report to IT Manager immediately. Isolate affected systems if necessary and follow cyber incident response procedures.
AI misuse linked to homework, assessment or NEA	Follow Homework Policy, AI Policy, JCQ/NEA guidance and malpractice procedures as applicable. (Currently Assistant Headteacher)
Staff misuse	Report to Headteacher/DSL as appropriate. Follow Staff Code of Conduct, low-level concerns, allegations and disciplinary procedures.

The school will consider whether incidents involving illegal activity, indecent images, AI-generated sexual imagery, threats, blackmail, extremist material, serious harassment, data breaches or cyber-crime should be reported to police, social care, Prevent, the LADO, the ICO, NCSC or other external bodies.

17. Training and professional development

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

monitoring responsibilities, reporting routes, cyber-bullying, radicalisation, online sexual abuse, child-on-child abuse, AI-related risks, data protection and acceptable use.

Training will ensure staff understand that technology is a significant component in many safeguarding and well-being issues and that children may experience online abuse through content, contact, conduct and commerce risks. Training will also help staff recognise emerging risks such as AI-generated sexual imagery, deepfakes, voice cloning, phishing, scams, impersonation and misinformation.

Governors will receive training on safe internet use, online safeguarding, filtering and monitoring, and AI-related safeguarding governance as part of their safeguarding training.

18. Monitoring, review and governance

The DSL and Online Safety Officer will maintain records of online safety incidents and review themes and trends. The policy will be reviewed annually by the Online Safety Officer and shared with the governing board. The review will be supported by an annual risk assessment that considers and reflects the risks pupils face online.

The annual review should include:

- effectiveness of filtering and monitoring systems;
- patterns in online safety incidents and pupil voice;
- emerging risks including AI, apps, games, platforms, scams and local safeguarding concerns;
- staff training and confidence;
- governor oversight and challenge;
- parent/carer engagement;
- curriculum coverage and adaptation for vulnerable pupils and pupils with SEND;
- review of approved digital and AI tools, including whether they remain safe, useful and compliant.

19. Links with other policies

- Child Protection and Safeguarding Policy
- Artificial Intelligence Policy
- Behaviour Policy
- Anti-Bullying Policy
- Staff Code of Conduct
- Data Protection Policy and privacy notices
- ICT and Internet Acceptable Use Policy
- Homework Policy
- Teaching and Learning Policy
- Assessment, NEA and Examinations Policies
- Searching, Screening and Confiscation / Behaviour procedures
- Complaints Procedure
- Low-Level Concerns and Allegations procedures

Appendix 1: pupil acceptable use agreement

I will use the school's ICT systems, internet, online platforms and approved digital tools safely, responsibly and respectfully. I understand that the school may monitor use of school systems to help keep everyone safe.

- I will only use school systems for school-related learning and activities.
- I will not try to access, create, share or search for illegal, inappropriate or harmful content.

- I will not use technology to bully, harass, threaten, impersonate, humiliate or exclude others.
- I will not create, request, possess, share or threaten to share nude, semi-nude, sexualised, violent, hateful or humiliating images of anyone, including AI-generated or edited images.
- I will not use AI tools in school unless a teacher has clearly said I may use them for a specific task.
- I will not use AI to complete work dishonestly, fake evidence, impersonate someone, bypass safety systems or create harmful content.
- I will not share my passwords or use another person's account.
- I will not record, photograph or livestream others without permission.
- I will report anything online that worries, upsets or harms me or someone else, even if I am worried that I have made a mistake.

Student name: _____ Form: _____ Signature: _____
Date: _____

Appendix 2: parent/carer acceptable use acknowledgement

I have discussed the school's expectations for safe, responsible and respectful use of technology with my child. I understand that the school may monitor use of school systems and will respond to misuse in line with safeguarding and behaviour procedures.

Parent/carer name: _____ Signature: _____ Date: _____

Appendix 3: acceptable use agreement for staff, governors, volunteers and visitors

When using the school's ICT systems, accessing the internet in school, using a work device, using a school account or using online/AI tools for school-related work, I will not:

- access, attempt to access, create, share, link to or send inappropriate, illegal, violent, extremist, pornographic, hateful or harmful material;
- use systems in a way that could harm pupils, staff, the school community or the school's reputation;
- install unauthorised software or connect unauthorised hardware/devices to the school network;
- share my password, use another person's account or leave accounts/devices unsecured;
- take, store or share photographs, video or audio of pupils except in line with school procedures and permissions;
- share confidential information about the school, pupils, staff, families or members of the community;
- access, modify, share or upload data I am not authorised to use;
- enter personal, sensitive, confidential, safeguarding or identifiable pupil information into unapproved AI tools;
- use AI tools to make automated decisions about pupils or to produce unchecked communications, assessments or records;
- use AI or online tools to create, edit or manipulate images, audio or video of pupils, staff or others in an inappropriate, misleading or harmful way;
- promote private business unless directly related to an authorised school purpose.

I will report online safety concerns, safeguarding concerns, filtering/monitoring failures, data breaches, cyber security concerns and AI-related concerns promptly through the appropriate school route. I will always use the school's ICT systems, internet and approved digital tools responsibly, and ensure that pupils in my care do so too.

Name: _____ Role: _____ Signature: _____ Date: _____

Appendix 4: online safety training needs self-audit for staff

Question	Yes/No	Comments/training need
Do you know who has lead responsibility for online safety in school?		
Do you understand your role in filtering and monitoring?		
Do you know how to report a filtering or monitoring failure?		
Are you aware of the ways pupils can abuse their peers online?		
Do you know what to do if a pupil reports an online safety concern?		
Do you understand the risks of nudes, semi-nudes, deepfakes, nudification and AI-generated sexual imagery?		
Do you understand what data must not be entered into unapproved AI tools?		
Are you familiar with the AI Policy and acceptable use expectations?		
Do you know how to set safe online homework resources and URLs?		
Do you know how to report phishing, scams or suspicious emails?		
Are there areas of online safety or AI safety where you would like further training?		

Appendix 5: online safety incident log

Date	Where/how incident took place	Description	Risk category	Action taken	Logged by
			Content / Contact / Conduct / Commerce / AI / Cyber / Data		

Appendix 6: filtering, monitoring and AI safety review checklist

Check	Evidence / action
Roles and responsibilities for filtering and monitoring are assigned and understood.	
Filtering and monitoring systems have been reviewed within the last 12 months.	
Staff know how to report blocked resources, unsafe access and monitoring failures.	
Pupil safeguarding risks, including AI-related risks, have informed the annual online safety risk assessment.	
Approved digital and AI tools have been checked for age suitability, privacy, data handling, security and safeguarding controls.	
Pupil-facing AI use is supervised and uses tools with appropriate safeguards.	
Cyber security arrangements have been reviewed, including phishing and AI-generated scam risks.	
Governors have received sufficient information to challenge and assure themselves of online safety arrangements.	

Appendix 7: AI/digital tool pre-use risk assessment prompt

Before staff promote or use a new AI or significant online tool with pupils, the following questions should be considered with the Online Safety Officer, DSL, IT Manager and/or Data Protection Officer as appropriate:

- What educational or workload benefit is the tool intended to deliver?
- Is the tool staff-facing only or pupil-facing?
- Is it age appropriate and compatible with school policy?
- What personal data, pupil work, images, voice, video or confidential information would be processed?

- Where is data stored and processed, and is there a lawful basis and privacy information?
- Does the tool use input data for model training or onward sharing?
- What filtering, monitoring, content moderation and safeguarding alert features exist?
- Can administrators set permissions, disable unsafe features and manage accounts?
- What are the risks of inaccurate, biased, harmful or inappropriate outputs?
- What supervision, staff training and pupil instruction are required?
- How will incidents, errors or concerns be reported and reviewed?
- Is a DPIA, procurement review or data-sharing agreement required?

Reference points used in this update

- Keeping children safe in education 2025, Department for Education.
- Keeping children safe in education 2026 consultation/draft proposals, Department for Education.
- Generative artificial intelligence (AI) in education, Department for Education, updated August 2025.
- Generative AI: product safety expectations, Department for Education, January 2025.
- Filtering and monitoring standards for schools and colleges, Department for Education.
- Cyber security standards for schools and colleges, Department for Education.
- Education inspection framework and State-funded school inspection toolkit, Ofsted, for use from November 2025.
- UKCIS guidance on sharing nudes and semi-nudes: advice for education settings.
- NCA/IWF professional guidance and current safeguarding warnings on AI-generated child sexual abuse material and sextortion.