Chesham House School Online Safety Policy

Rebecca Smith – DSL

Email: rebecca.smith@cambiangroup.com

Alice Mullen – DDSL

Email: alice.mullen@cambiangroup.com

At Chesham House School, our online safety lead is Jo Williams, deputy headteacher.

1. Purpose

Our school recognises the benefits and risks of technology use among children and students.

This policy aims to:

- Safeguard individuals from harmful or inappropriate online content
- Promote a whole-school approach to online safety
- Balance access control with education on responsible use
- Empower individuals to make safe decisions and report concerns
- Ensure staff understand online-safety practices and manage their online presence in a professional manner.

An effective whole school approach to online safety empowers, protects and educates children and students in their use of technology and establishes mechanisms to identify, intervene in, and escalate any concerns where appropriate.

2. Legislative Context

This Policy is underpinned by a range of statutory and regulatory frameworks which ensure our children and students are protected from harm and risks arising from digital technologies. They include:

Keeping children safe in education 2025

Teaching online safety in schools - GOV.UK

Online safety (e-safety) and schools | NSPCC Learning

Working together to safeguard children 2023: statutory guidance

3. Background

Technology is integral to modern life and learning. Safe internet access is not a luxury but a right for all individuals.

However, despite the many benefits technology brings, our school is alert to its' potential risks which include:

- Exposure to illegal/inappropriate content
- Data breaches and privacy violations
- Grooming, radicalisation, and extremist content
- Cyberbullying and inappropriate contact
- Misuse of personal images/videos

- AI associated harm
- Misinformation, disinformation and conspiracy theories
- Plagiarism, copyright infringement, and illegal downloads
- Excessive use affecting wellbeing
- Being used as a tool to perpetrate online abuse such as harassment, stalking, sharing indecent images, sexual exploitation, grooming, and inciting sexual activity

Taking the above into consideration, online safety is embedded within the broader safeguarding framework and should be read alongside relevant associated safeguarding policies as outlined in the 'legislative context' section of this policy.

Our staff are aware that resilience is key to mitigating online risks and work hard to equip children and students with knowledge and skills required to keep themselves safe online.

4. Roles and Responsibilities

Designated Safeguarding Lead (DSL)

- Leads on safeguarding and online safety
- Oversees incident logs, filtering & monitoring systems, and staff training
- Is trained in online safety and understands risks including grooming, radicalisation, online abuse and AI.

Head of Service

- Ensures safety of individuals and staff
- Provides CPD for staff on online safety
- Monitors internal safety roles and reports to governance board

Senior Leadership Team

- Manages daily online safety issues
- Reviews policies and incidents
- Liaises with IT, Local Authority, and external agencies

Information Governance and IT Leaders / Technical Staff

- Maintains secure infrastructure and filtering systems
- Monitors network/VLE/email use
- Implements and updates monitoring software
- Ensures wireless access is proactively managed and secured

All Staff

- Stay informed on online safety and peer-on-peer abuse
- Follow the Acceptable Use Policy (GIG 18 Policy)
- Report concerns to the Online Safety Lead
- Maintain professional communication via official systems
- Embed online safety in curriculum and activities
- Never share login credentials
- Monitor device use and internet access

Parents/Carers

- Play a key role in promoting safe technology use
- Our school/college supports parents via newsletters, events and campaigns

5. Teaching and Learning

Individuals are given clear objectives, taught acceptable use and guided in evaluating online materials.

Our school:

- Complies with copyright laws
- Provides age-appropriate access
- Maintains virus protection and system security
- Ensures password management and IT security align with the Prevent Policy

6. Use of Email

Staff use work-provided email accounts for all official communication. This protects confidentiality and staff from allegations.

7. Website

Our website only publishes location contact details (address, email, phone) and does not publish personal information of staff or individuals will be shared. All content is accurate, appropriate, and complies with privacy and copyright policies. No photographs of children or students are uploaded or shared without appropriate consent.

8. Internet Use

- Inappropriate website content is reported immediately
- Parents/carers are informed that internet access is supervised
- Every individual has a personalised online safety risk assessment that is reviewed regularly in line with care and education planning
- Our school has robust filtering and monitoring systems in place, however, staff are aware that mobile devices with wireless access can bypass these systems – staff remain alert to any signs of concern

9. Social Networks

Teaching staff deliver lessons on social networking safety, covering areas such as the risks of uploading personal content and challenges removing content once shared.

Lessons also focus on privacy and the risks surrounding sharing personal details. This is pitched to children and students' development and level of understanding.

10. Staff and Volunteers

- Follow the GHR 37 Code of Conduct and Teams Etiquette Guide
- Raise concerns about inappropriate use
- Follow the Whistleblowing, Child Protection and other associated policies
- Immediately reporting concerns when they arise
- Maintain confidentiality and involve parents/carers when appropriate

11. Sexting (Sharing Nudes and Semi-Nudes)

Sexting, also known as the sharing of nudes or semi-nudes, involves sending or receiving sexually explicit images, videos, or messages via digital devices. While often perceived as harmless, it is illegal for anyone under 18 to create, share, or possess such content—even if consensual. Young people may engage in sexting for reasons such as peer pressure, curiosity, or self-esteem, but they often underestimate the risks, including loss of control over images, exposure to exploitation, bullying, and emotional distress. Once shared, content can be copied, distributed, or accessed by unknown individuals, including sex offenders.

Staff must respond to disclosures calmly and follow safeguarding procedures immediately. This involves notifying the DSL immediately. The National Police Chief's Council (NPCC) advises that safeguarding—not criminalisation—should be the priority. If the incident involves coercion, violence, or individuals under 13 or over 18, police and children's social care must be contacted**.** If a child is in immediate danger, call 999 or NSPCC at 0808 800 5000. Staff should avoid viewing the content and isolate devices if necessary. All actions must be recorded, and if a child is in immediate danger, emergency services must be contacted without delay

12. Use of Digital Images and Videos

- Staff educate individuals on risks of sharing images
- Staff only use school equipment for capturing images
- Staff ensure individuals are appropriately dressed prior to taking an image
- Full names are avoided in published photos
- Images are carefully selected and follow best practice guidance

13. Cyberbullying

- Cyberbullying is persistent, anonymous, and harmful
- Common forms include texts, images, emails, chat rooms, IM, websites
- Cyberbullying can reach large audiences quickly and anonymously
- Most incidents involve peers within the same class or year group
- Despite lack of physical evidence, cyberbullying can be deeply harmful

- Our school supports victims and educates staff and individuals on prevention and reporting
- Regular parent/carer sessions are held on cyberbullying and online child protection

14. Emerging Technology - AI

Our school evaluates emerging technology for suitability before use. AI-generated content is now recognised as a potential online safety risk. Our school is aware that children/students may encounter misinformation, disinformation, or harmful outputs from AI tools — even those used in educational settings. Filtering and monitoring systems are reviewed to account for AI risks and our digital safety infrastructure is in line with the new DfE guidance/tool 'Plan Technology for Your School'.

Our Designated Safeguarding Leads (DSLs) are alert to AI-related risks including how AI tools might be used to bypass filters, spread conspiracy theories, or deliver content that appears trustworthy but is inaccurate or harmful.

Our school staff are trained in AI risks so they can identify and respond to any emerging concerns.

15. Management of Information Systems

All systems are managed according to the Information Security Policy. Virus protection is updated daily and robust filtering and monitoring systems are in place. Unsuitable sites are blocked immediately, servers are secured, access is restricted and files are checked for malware. Software is installed by IT technicians and staff never share assigned devices or login credentials. Wireless access is proactively managed and secured.

16. Students aged 18 years and Over

Online safety responsibilities extend to students aged 18 and over, especially those who may be vulnerable due to trauma, learning disabilities, mental health conditions, or other needs. Although legally classified as adults, these individuals may still

require tailored safeguarding measures, including supervised access to technology, individualised risk assessments, and ongoing education around online safety.

Staff are alert to signs of online abuse, exploitation, or coercion, and where there are concerns about an individual's ability to make informed decisions, staff follow the Over 18s Safeguarding Policy and arrange for Mental Capacity Act (MCA) assessments where appropriate. In such cases, decisions are made in the individual's best interests, ensuring that support and restrictions are proportionate, protective, and respectful of individual rights.

Review History

A review will be undertaken annually as a minimum. However, subject to a significant safeguarding concern this policy and all other attached policies will be reviewed and monitored as part of a lessons learned review.

This policy was reviewed in August 2025 by Laura Dickie (Head of Policy), Kate Brogan (Head of IT), Russell Edge (Senior Information Risk Owner), Rebecca Smith (headteacher/DSL) and agreed by the Head of the Governance Board.

Next Review – September 2026