



Online Safety Policy

August 2026

Document Quality Control

Original

Version	Author	Date	Reviewed By	Date
Version 1	Lisa Morton	May 2022	Gareth Collier	May 2022

Document Reviews/Updates

Document Version Editing	Reason for Review/Update	Reviewer	Date	Checked / Approved By	Date
002	CSFC Cam opening	GT	01/08/22	GC	08/08/22
003	CSFC Cam Review	GT	07/01/23	JD	10/01/23
004	CSFC Cam Review	GT	06/09/23	JD	06/09/23
005	CSFC Cam Review	GT	16/09/24	JD	16/9/24
006	CSFC Cam Review	CCD	15/09/25	JD	18/9/25
007	CSFC Cam Review	CCD	16/12/25	JD	16/12/25
008	CSFC Cam Review	CCD	01/08/26	JD	18/08/26

Contents

1. Introduction	3
2. Statutory and Non-Statutory Guidance	3
3. Policy Scope	4
4. The Four Cs of Online Safety	4
4.1 Content – What students see online	4
4.2 Contact – Who students interact with online	5
4.3 Conduct – How students behave online	5
4.4 Commerce – Online financial risks	5
5. Roles and Responsibilities	6
5.1 Designated Safeguarding Lead (DSL)	6
5.2 Staff	6
5.3 Students	6
6. Filtering, Monitoring and Security	7
7. Use of Images and Video	8
8. Responding to Online Safety Incidents	8
9. Training, Awareness and Education	9
10. Monitoring and Review	9
Appendix 1	10
E-Safety Incident Reporting Procedure Flowchart	10

1. Introduction

This Online Safety Policy should be read alongside the College's Safeguarding and Child Protection Policy, ICT Acceptable Use Policy, Anti-Bullying Policy, Prevent Policy, PSHE and RSE Policies, Staff Handbook, Student Handbook, Search, Screening and Confiscation and Use of Physical Intervention Policy, Data Protection Policy and Good Behaviour and Sanctions Policy.

Cardiff Sixth Form College Cambridge recognises the significant educational benefits and opportunities offered by digital technologies, online platforms, artificial intelligence (AI) and internet access. These technologies play a vital role in teaching, learning, communication and preparation for adult life. However, the College also recognises that online activity presents safeguarding risks that require robust systems, effective education and a strong safeguarding culture.

The College is committed to ensuring that students and staff use technology safely, responsibly, lawfully and confidently. Online safety is an integral part of safeguarding and forms part of the College's wider duty of care. The College recognises that many safeguarding concerns can occur both online and offline, and that these risks are often interconnected.

The College adopts a whole-college approach to online safety. Online safety is embedded within safeguarding procedures, staff training, filtering and monitoring arrangements, curriculum planning, PSHE and RSE provision, assemblies, tutorials and pastoral programmes. The College actively promotes Safer Internet Day and wider online safety awareness initiatives throughout the academic year.

2. Statutory and Non-Statutory Guidance

This policy reflects current statutory requirements and national guidance, including:

- Keeping Children Safe in Education (DfE, 2026)
- Teaching Online Safety in Schools (DfE)
- Filtering and Monitoring Standards for Schools and Colleges (DfE)
- Meeting Digital and Technology Standards in Schools and Colleges (DfE)
- Sharing Nudes and Semi-Nudes: Advice for Education Settings (DfE)
- Searching, Screening and Confiscation (DfE)
- UK Safer Internet Centre guidance
- Prevent Duty Guidance
- Relevant Information Commissioner's Office (ICO) guidance relating to children's data and online privacy.

3. Policy Scope

This policy applies to:

- All students, staff, governors, volunteers and visitors
- All use of College IT systems, networks and devices
- Personal devices used on College premises or networks
- Online activity undertaken off-site where it impacts safeguarding, welfare or the reputation of the College

Students are required to read and sign the ICT Acceptable Use Policy during induction.

4. The Four Cs of Online Safety

The College structures its approach to online safety using the **Four Cs framework: Content, Contact, Conduct and Commerce**, as referenced in KCSIE.

4.1 Content – What students see online

Risks may include:

- Exposure to illegal, harmful or inappropriate content, including pornography, violent content, self-harm, suicide, extremism and radicalisation
- Misinformation, disinformation, conspiracy theories and manipulated media
- Harmful online trends or challenges
- Unregulated or misleading content generated by artificial intelligence (AI)

The College will:

- Use appropriate filtering and monitoring systems to reduce exposure to harmful content
- Educate students to critically evaluate online information and sources
- Teach digital literacy, including the ethical, safe and responsible use of AI
- Encourage students to report concerning online content

Generative Artificial Intelligence (AI)

Generative AI tools are capable of producing text, images, audio, video and other content in response to user prompts. Whilst these technologies offer significant educational benefits, they also present safeguarding, wellbeing and academic integrity risks.

Potential risks include:

- Exposure to inaccurate, biased or misleading information presented as fact
- Generation of inappropriate, sexualised, violent or extremist content
- Creation of deepfake images, audio or video
- Impersonation of students, staff or other individuals
- Academic malpractice through inappropriate reliance on AI

- Students becoming overly reliant upon AI or using AI chatbots as a substitute for appropriate adult support

The College will:

- Educate students about how generative AI works and its limitations
- Teach students to critically evaluate AI-generated content
- Promote ethical and responsible use of AI in accordance with academic integrity expectations
- Treat misuse of AI, including the creation or sharing of harmful, deceptive or abusive content, as a safeguarding and/or disciplinary matter where appropriate

4.2 Contact – Who students interact with online

Risks may include:

- Online grooming, sexual exploitation and sextortion
- Coercion, manipulation or emotional abuse
- Radicalisation and exposure to extremist ideologies
- Contact with unknown adults or individuals seeking to exploit young people

The College will:

- Educate students about healthy online relationships and appropriate boundaries
- Reinforce that students should never feel pressured to share personal information, passwords or images
- Promote awareness of CEOP, Thinkuknow and other reporting routes
- Respond promptly to concerns in accordance with safeguarding procedures

4.3 Conduct – How students behave online

Risks may include:

- Cyberbullying and online harassment
- Image-based abuse, including the creation, possession or sharing of nude or semi-nude images
- Creation or sharing of deepfake or manipulated content intended to cause harm
- Hate speech, discrimination or abusive behaviour
- Damage to personal reputation and digital footprint

The College will:

- Promote respectful, responsible and lawful online behaviour
- Address online bullying through the Anti-Bullying and Safeguarding Policies
- Apply appropriate sanctions where behaviour breaches College expectations
- Support students in understanding the long-term consequences of online behaviour

4.4 Commerce – Online financial risks

Risks may include:

- Online scams, phishing and fraud
- Gambling and gaming-related financial harm
- Exploitative advertising and in-app purchases
- Cryptocurrency scams and high-risk financial schemes

The College will:

- Educate students to recognise and avoid online financial risks
- Encourage caution when sharing personal or financial information online
- Support students who may be affected by online exploitation or fraud
-

5. Roles and Responsibilities

5.1 Designated Safeguarding Lead (DSL)

The DSL has overall responsibility for online safety and will:

- Act as the lead professional for online safety concerns
- Ensure incidents are recorded and managed in line with safeguarding procedures
- Liaise with external agencies such as Children's Services, Police and CEOP where required
- Keep up to date with emerging online risks and guidance
- Provide staff with relevant training and updates

The DSL will also liaise with the Safeguarding Governor and Senior Leadership Team (SLT).
The Safeguarding Governor is also the Online Safety Governor

5.2 Staff

All staff:

- Have a duty to safeguard students and report concerns immediately to the DSL
- Must not promise confidentiality
- Are expected to model safe and professional online behaviour
- Must use College systems in accordance with the ICT Acceptable Use Policy
- May only communicate with students via College-approved platforms

Teaching staff are responsible for reinforcing online safety messages within their subject areas.

Staff should remain professionally curious where online behaviour or activity may indicate wider safeguarding concerns.

5.3 Students

Students are expected to:

- Use College IT systems responsibly and safely
- Follow the ICT Acceptable Use Policy and other relevant policies
- Report concerns about online safety involving themselves or others
- Act responsibly online, including outside College hours where behaviour impacts safeguarding or welfare

Students are encouraged to report harmful online content or behaviour, even where they are not directly involved.

6. Filtering, Monitoring and Security

The College provides a safe online environment through appropriate filtering and monitoring systems, in accordance with *Keeping Children Safe in Education* and the Department for Education's *Meeting digital and technology standards in schools and colleges: Filtering and Monitoring Core Standard*.

The College recognises that filtering is preventative and is intended to restrict access to illegal, inappropriate and potentially harmful online content, while monitoring is reactive and enables potentially concerning online activity to be identified, reviewed and acted upon. Filtering and monitoring systems support, but do not replace, effective staff supervision, professional judgement and safeguarding practice.

The Board of Governors has overall strategic responsibility for ensuring that appropriate filtering and monitoring arrangements are in place and that the relevant standards are met. A member of the Senior Leadership Team has responsibility for overseeing the College's filtering and monitoring arrangements (Clair Curtis-Dyke, Vice Principal Pastoral and Boarding). The Designated Safeguarding Lead (DSL) leads on safeguarding and online safety, including reviewing relevant monitoring reports and responding to safeguarding concerns identified through filtering and monitoring. IT support is responsible for the technical maintenance, operation and testing of the systems and for providing appropriate reports and information to senior leaders and the DSL.

The College ensures that:

- filtering systems are appropriate to the age, needs and risk profile of students and do not unreasonably restrict teaching, learning or legitimate College activity;
- filtering is applied appropriately to College-managed devices, including devices used away from the College site, and to users accessing the College network;
- different levels of access can be applied where appropriate, including separate filtering profiles for students and staff;
- filtering systems are designed to restrict access to illegal and harmful content and are kept active and up to date;
- appropriate measures are in place to reduce attempts to circumvent filtering, including through VPNs, proxy services or other technologies;
- monitoring arrangements enable potentially harmful, inappropriate or illegal activity to be identified and escalated promptly;
- monitoring reports highlighting incidents are reviewed at least weekly, with high-risk safeguarding, malicious or technical incidents reported immediately;
- all staff understand their responsibilities for monitoring students' use of technology and know how to report safeguarding or technical concerns;

- staff provide appropriate in-person supervision when students are using digital devices;
- relevant incidents, actions taken and outcomes are recorded;
- users are informed that filtering and monitoring arrangements are in place; and
- data collected through monitoring is handled in accordance with data protection legislation, relevant privacy notices and, where required, a Data Protection Impact Assessment.

Filtering and monitoring provision is formally reviewed at least once every academic year by appropriate members of the Senior Leadership Team, the DSL and IT support, with oversight from the Board of Governors. The review considers the College's student risk profile, safeguarding incidents and intelligence, curriculum requirements, use of College and personal devices, changes in technology and working practices, and the effectiveness and limitations of existing systems.

The review specifically considers emerging technologies, including generative artificial intelligence, real-time and dynamically generated content, personalised content and any technologies that may reduce the effectiveness of existing filtering or monitoring controls.

Additional reviews are undertaken where appropriate, including following a significant safeguarding concern, the introduction of new technology or devices, significant software or network changes, or changes to working practices.

The College undertakes and records appropriate checks of its filtering and monitoring systems. Annual auditing will be conducted by college and monitored by Governors. These checks consider both safeguarding and technical effectiveness and include confirmation that systems remain active, are correctly configured for relevant user groups and operate effectively across College-managed devices and locations. Records identify when checks were undertaken, by whom, what was checked or tested and any resulting actions.

Filtering and monitoring arrangements complement, but do not replace, effective staff vigilance, appropriate classroom supervision and the responsibility of all staff to identify and report safeguarding concerns.

7. Use of Images and Video

The College recognises the educational value of images and video but also the safeguarding risks.

- Use of images must comply with data protection and consent requirements
- Students and staff are educated on risks associated with sharing personal images
- Image-based abuse is treated as a safeguarding concern
- Parental consent for use of student images is obtained during admissions

The unauthorised use of **smart glasses, wearable recording devices or other covert recording technology** is prohibited on College premises.

8. Responding to Online Safety Incidents

All online safety incidents are treated seriously.

- Reports may be made to any member of staff

- Staff must follow safeguarding procedures immediately
- The College will take proportionate action to prevent harm
- External agencies may be involved where appropriate

Sanctions will be applied in line with College policies. Serious incidents will be managed by the DSL and SLT.

Where an incident constitutes, or may constitute, abuse, the College will manage the matter in accordance with the Safeguarding and Child Protection Policy and work with external agencies where appropriate.

9. Training, Awareness and Education

- Online safety training is provided to staff regularly
- Students receive age-appropriate education through PSHE, RSE, assemblies and pastoral provision
- Key resources are signposted, including:
 - www.saferinternet.org.uk
 - www.thinkuknow.co.uk

All staff receive online safety training as part of safeguarding induction and through regular safeguarding updates to ensure awareness of emerging technologies and online risks.

10. Monitoring and Review

This policy is reviewed annually by the Senior Leadership Team, Designated Safeguarding Lead and Safeguarding Governor, or sooner if:

- National guidance changes
- A significant incident occurs
- Emerging risks are identified

This ensures continuous improvement and alignment with safeguarding best practice.

Appendix 1

E-Safety Incident Reporting Procedure Flowchart

