CARDIFF SIXTH FORM COLLEGE

CAMBRIDGE

E-Safety Policy

December 2025

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

Contents

Cardiff Sixth Form College, Cambridge

1. Introduction

This E-Safety and 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, Screen and Confiscate and Use of Physical Intervention Policy, Data Protection Policy, and the Good Behaviour and Sanctions Policy.

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

The College is committed to ensuring that students and staff can use technology safely, responsibly and confidently. Online safety is an integral part of the College's safeguarding responsibilities and wider duty of care, and is embedded within PSHE and RSE provision, assemblies, tutorials and pastoral programmes. The College actively promotes Safer Internet Day and wider online safety awareness initiatives.

2. Statutory and Non-Statutory Guidance

This policy reflects current statutory requirements and best practice guidance, including:

- *Keeping Children Safe in Education* (DfE, 2024/2025)
- *Teaching Online Safety in Schools and Colleges* (DfE, updated 2023)
- *Enhancing Digital Resilience in Education* (DfE, 2021)
- *Sharing Nudes and Semi-Nudes: Advice for Education Settings* (DfE)
- NSPCC *E-Safety for Colleges* (updated January 2024)
- UK Safer Internet Centre guidance
- Prevent Duty Guidance

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 harmful, illegal or inappropriate content (e.g. pornography, violence, extremism, self-harm)
- Misinformation, disinformation and fake news
- Harmful online challenges or trends
- Unregulated or misleading content generated by artificial intelligence (AI)

The College will:

- Use 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 and safe use of AI tools
- Encourage reporting of concerning content

Generative Artificial Intelligence (AI) Generative AI tools are able to create text, images, audio, video and other content in response to user prompts. While these tools can support learning, creativity and accessibility, they also present online safety and safeguarding risks.

Potential risks associated with generative AI include:

- Exposure to inaccurate, biased or misleading information presented as fact
- Creation or access to inappropriate, sexualised, violent or extremist content
- Use of AI to impersonate others, including staff or students
- Generation of deepfake images, video or audio
- Over-reliance on AI that undermines independent learning or academic integrity

The College will:

- Educate students about what generative AI is and how it works
- Teach students to critically evaluate AI-generated content and verify information
- Set clear expectations for the ethical and appropriate use of AI in learning, in line with academic integrity policies
- Treat misuse of AI, including the creation or sharing of harmful or deceptive content, as a safeguarding or disciplinary matter where appropriate

4.2 Contact – Who students interact with online

Risks may include:

- Online grooming and sexual exploitation
- Coercion, pressure or manipulation
- Radicalisation and exposure to extremist ideologies
- Unsupervised contact with adults or unknown individuals

The College will:

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

4.3 Conduct – How students behave online

Risks may include:

- Cyberbullying and online harassment
- Image-based abuse, including the sharing of nudes and semi-nudes
- Hate speech or discriminatory behaviour
- Damage to digital reputation and online footprints

The College will:

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

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 and high-risk financial schemes

The College will:

- Educate students on recognising and avoiding online financial risks
- Encourage caution when sharing personal or financial information
- 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).

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.

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

6. Filtering, Monitoring and Security

The College employs appropriate filtering and monitoring systems to safeguard users. These systems:

- Are proportionate and reviewed regularly
- Support safeguarding rather than replace professional judgement
- Flag potential concerns to senior staff and the DSL

All digital activity on the College network may be monitored in line with data protection legislation and safeguarding obligations.

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

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.

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

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