



Online safety Policy

Aspire • Believe • Achieve

Staff member responsible:	Hazel McCalvey
Role:	Deputy Head (Academic)
Revised On:	Sept 2026
Ratified by governing board:	
Review Due:	Sept 2027

Introduction

Frewen College adopts a whole-College approach to safeguarding. Safeguarding is the golden thread that runs throughout every aspect of College life and underpins all policies, procedures and practices. Online safety is a key component of this approach and is recognised as a safeguarding issue that requires effective leadership, governance, education and risk management.

Oversight and implementation of this policy rests with Heather Miller, the designated Safeguarding Governor, who is responsible for monitoring the effectiveness of safeguarding arrangements, including online safety, on behalf of the Board of Governors. Heather Miller can be contacted through the College.

Scope and Purpose

All staff, governors, volunteers, contractors and any individual providing services on behalf of the College have a responsibility to understand and implement this policy, both during and outside normal College hours, including educational visits, residential activities and off-site provision.

All new employees and volunteers are required to confirm that they have read, understood and will comply with this policy and associated procedures as part of the induction process.

This responsibility is particularly important in relation to the Prevent Duty, as radicalisation frequently occurs through online platforms, social media and digital communications. Staff must remain vigilant and follow the procedures contained within the Safeguarding and Child Protection Policy and Preventing Extremism and Tackling Radicalisation Policy where concerns arise.

The purpose of this policy is to safeguard students and staff through the promotion of safe, responsible and effective use of technology. It establishes clear expectations regarding behaviour, monitoring, reporting and education in order to maintain a safe digital environment.

Online safety is an interrelated and running theme throughout the College's safeguarding arrangements and wider policies. The Staff and Student Acceptable Use Policies (AUPs) form an integral part of this policy and should be read alongside it.

Statutory Basis

This policy should be read alongside:

- Keeping Children Safe in Education (KCSIE) (DfE: currently in force);
- Working Together to Safeguard Children (currently in force);
- Relationships Education, Relationships and Sex Education (RSE) and Health Education statutory guidance;
- Teaching Online Safety in Schools (DfE);
- DfE Digital and Technology Standards for Schools and Colleges;
- DfE Filtering and Monitoring Standards;
- DfE Cyber Security Standards;
- Education for a Connected World Framework;
- Independent School Standards Regulations;
- Independent School Standards Guidance (April 2026);
- UK GDPR and the Data Protection Act 2018.

Online safety is recognised as a safeguarding issue and forms an integral part of the College's whole-college safeguarding culture and approach.

Compliance Mapping

This policy supports compliance with:

- Keeping Children Safe in Education (KCSIE) (currently in force), including online safety, filtering and monitoring, child-on-child abuse, cyber security and digital safeguarding requirements.
- Meeting Digital and Technology Standards in Schools and Colleges, including the Filtering and Monitoring Standards and Cyber Security Standards.
- Independent School Standards Guidance April 2026, including Part 3 (Welfare, Health and Safety), Part 6 (Provision of Information), Part 7 (Complaints) and Part 8 (Leadership and Management).
- Teaching Online Safety in Schools and Education for a Connected World.
- UK GDPR and the Data Protection Act 2018.

The Board of Governors, Headmaster and senior leaders will use this policy as part of the College's wider safeguarding and quality assurance framework to demonstrate compliance with statutory safeguarding and independent school requirements.

Legal Status

This policy complies with:

- The Education (Independent School Standards) (England) Regulations;
 - National Minimum Standards for Boarding Schools (where applicable);
 - Relevant safeguarding and data protection legislation currently in force.
-

Monitoring and Review

These arrangements are subject to continuous monitoring, review and audit by:

- The Headmaster;
- The Designated Safeguarding Lead (DSL);
- The IT Manager;
- The Safeguarding Governor.

The College will undertake a documented review of the effectiveness of its filtering and monitoring arrangements **at least once every academic year**.

The review will consider:

- Student accounts;
- Staff accounts;
- Guest accounts;
- Boarding provision;
- College-owned and authorised devices;
- Filtering effectiveness;
- Monitoring reports and alerts;
- Online safety incidents;
- Cybersecurity risks;
- Generative AI and emerging technologies;
- Deepfake and AI-generated content risks;
- Compliance with KCSIE and DfE Filtering and Monitoring Standards.

The findings, actions and outcomes of the review will be recorded in writing and reported to the Board of Governors. Any weaknesses identified will be addressed without delay.

The annual filtering and monitoring review will also assess whether filtering and monitoring controls remain effective across all internet-connected devices, user accounts, networks and locations used for College business, including boarding provision. The review will evaluate the effectiveness of safeguards relating to students, staff, visitors, remote access, authorised personal devices, artificial intelligence platforms and emerging technologies. Records of testing, findings, recommendations,

actions taken and subsequent impact will be retained by the College as evidence of compliance and continuous improvement.

Related Policies

This policy should be read alongside:

- Safeguarding and Child Protection Policy;
- Preventing Extremism and Tackling Radicalisation Policy;
- Staff Behaviour (Code of Conduct) Policy;
- Student Behaviour Policy;
- Anti-Bullying Policy;
- Mobile Phone and Personal Device Policy;
- Searching, Screening and Confiscation Procedures;
- IT Acceptable Use Policy (Staff);
- IT Acceptable Use Policy (Students);
- Cyber Security Policy;
- Data Protection Policy;
- Privacy Notices;
- Relationships and Sex Education (RSE) Policy;
- Artificial Intelligence and Generative AI Use Policy.

Filtering and Monitoring

The College is committed to providing a safe online environment for all users.

Filtering and monitoring are essential safeguarding measures which help protect students and staff from illegal, inappropriate or harmful material.

The Designated Safeguarding Lead and Safeguarding Governor work closely with the IT Manager to ensure that filtering and monitoring systems:

- Are appropriately procured and maintained;
- Reflect the needs of students including those with SEND;
- Take account of safeguarding risks such as exploitation, county lines activity, radicalisation and online abuse;
- Consider Bring Your Own Device (BYOD) arrangements;
- Are reviewed regularly and formally evaluated.

The College's systems aim to:

- Block illegal, harmful and inappropriate content;

- Avoid unreasonable over-blocking;
- Support teaching and learning;
- Generate effective safeguarding alerts;
- Support early intervention where concerns arise.

Filtering and monitoring arrangements apply to:

- Student accounts;
- Staff accounts;
- Guest accounts;
- Boarding environments;
- College-owned devices;
- Approved personal devices.

Records of reviews, audits and actions taken are maintained.

Artificial Intelligence (AI), Deepfakes and Emerging Technologies

The College recognises that artificial intelligence presents both educational opportunities and safeguarding risks.

Students and staff will receive guidance on:

- Generative AI systems;
- AI chatbots;
- Deepfakes;
- AI-generated imagery;
- Nudification applications;
- Misinformation and disinformation;
- Online manipulation and coercion;
- Identity theft and impersonation;
- Academic integrity and plagiarism;
- Ethical use of AI technologies.

The creation, possession, sharing or distribution of AI-generated intimate images involving children will be treated as a serious safeguarding concern and managed under the Safeguarding and Child Protection Policy.

All concerns relating to AI misuse must be reported to the Designated Safeguarding Lead immediately.

Roles and Responsibilities

Designated Safeguarding Lead (DSL)

The DSL has lead responsibility for online safety and digital safeguarding.

The DSL will:

- Support the Headmaster in implementing this policy;
- Work closely with the IT Manager and Safeguarding Governor;
- Ensure incidents are recorded and managed appropriately;
- Oversee responses to cyberbullying and online abuse;
- Deliver training for staff;
- Liaise with external agencies where required;
- Provide induction training to new staff;
- Report regularly to the Headmaster and Board of Governors;
- Oversee filtering and monitoring arrangements and annual reviews;
- Monitor emerging risks including AI, deepfake technology and online exploitation.

IT Manager

The IT Manager is responsible for:

- Day-to-day operation of filtering and monitoring systems;
- Network security;
- Cybersecurity measures;
- Technical investigations;
- Supporting safeguarding reviews;
- Advising senior leaders regarding emerging digital risks.

Safeguarding Governor

The Safeguarding Governor receives regular reports regarding:

- Online safety incidents;
- Filtering and monitoring effectiveness;
- Cybersecurity risks;
- AI-related concerns;
- Staff training;
- Findings from annual reviews.

The Safeguarding Governor provides challenge, scrutiny and oversight on behalf of the Board of Governors.

All Staff

All staff are responsible for:

- Remaining vigilant to online safeguarding concerns;
 - Following this policy and associated procedures;
 - Reporting concerns immediately to the DSL;
 - Maintaining professional conduct online;
 - Complying with the Staff Acceptable Use Policy;
 - Undertaking regular safeguarding and online safety training;
 - Understanding the risks associated with AI-generated content, online abuse, cyber security threats and radicalisation.
-

Parents and Carers

Parents are expected to:

- Raise concerns promptly with the College;
- Promote safe online behaviours at home;
- Engage with online safety guidance provided by the College;
- Support their child in complying with Acceptable Use Policies.

The College will continue to provide online safety information through newsletters, parent briefings, the College website and other communication channels.

Students

All students must:

- Sign and comply with the Student Acceptable Use Policy;
 - Use College systems responsibly;
 - Report concerns to a trusted adult;
 - Respect the rights, privacy and safety of others online.
-

Breadth of Online Safety Issues

The College recognises four broad categories of online risk:

Content

Exposure to harmful, illegal or inappropriate content including:

- Extremism;
- Racism;
- Misogyny;
- Self-harm content;
- Suicide content;
- Misinformation;
- Disinformation.

Contact

Harmful interactions including:

- Grooming;
- Exploitation;
- Radicalisation;
- Coercion;
- Online harassment.

Conduct

Behaviour that creates risk including:

- Cyberbullying;
- Sharing indecent images;
- Sexting;
- Online abuse;
- Unsafe social media use.

Commerce

Risks associated with:

- Fraud;
- Scams;
- Phishing;
- Financial exploitation;
- Online gambling.

Teaching About Online Safety

Online safety is delivered through:

- PSHE;
- RSE;
- Computing;
- Tutor programmes;
- Assemblies;
- Safeguarding education.

Students will be taught about:

- Healthy online relationships;
- Consent and boundaries online;
- Social media use;
- Online sexual harassment;
- Child-on-child abuse;
- Grooming and exploitation;
- Sexting and image sharing;
- Pornography and associated harms;
- Cyberbullying;
- Digital resilience;
- Misinformation and disinformation;
- Deepfakes;
- AI-generated content;
- Online scams;
- Critical evaluation of online information;
- Responsible use of artificial intelligence tools;
- Deepfake awareness and reporting;
- Identifying manipulated content;
- Online reputation and digital footprint management;
- Safe use of emerging technologies.

Cyber Security

The College recognises that cybersecurity is a safeguarding responsibility.

Cyber incidents can lead to:

- Loss of safeguarding information;
- Disclosure of personal data;
- Identity theft;
- Financial fraud;
- Online exploitation;
- Disruption to safeguarding systems.

Cyber incidents will therefore be assessed for safeguarding implications and referred to the DSL where appropriate.

The College follows DfE Digital and Technology Standards and Cyber Security Standards.

Privacy, Monitoring and Data Protection

The College operates filtering and monitoring systems as part of its safeguarding duty.

Users should understand that:

- Internet use on College systems may be monitored;
- Safeguarding alerts may be generated automatically;
- Browsing activity may be reviewed where concerns arise;
- Data will be processed in accordance with UK GDPR and the Data Protection Act 2018;
- Further information is available within the College Privacy Notices.

The College's Privacy Notices explain how browsing data, filtering reports, monitoring alerts and safeguarding records are collected, stored, accessed, shared and retained. Monitoring information will only be accessed by authorised staff where necessary to fulfil safeguarding, welfare, behaviour, legal or cybersecurity responsibilities.

The College seeks to balance safeguarding duties, privacy rights and educational needs appropriately.

Complaints Relating to Online Safety

Concerns relating to online safety, filtering, monitoring, cybersecurity or digital safeguarding should be raised through the following process:

1. Designated Safeguarding Lead;
2. Headmaster;
3. College Complaints Procedure.

Safeguarding concerns will be managed in accordance with the Safeguarding and Child Protection Policy.

Mobile Electronic Devices

Students must comply with the Mobile Phone and Personal Device Policy.

The searching, screening, confiscation and return of devices will be undertaken in accordance with:

- KCSIE (currently in force);
- Mobile Phone and Personal Device Policy;
- Behaviour Policy;
- Searching, Screening and Confiscation Procedures.

Any safeguarding concerns identified through a device search will be referred immediately to the DSL.

All searches of electronic devices will be conducted proportionately, lawfully and in accordance with statutory guidance. The College will consider safeguarding, privacy and welfare implications when determining any action arising from the search of a device.

The unauthorised photographing, filming, recording, livestreaming or sharing of images involving members of the College community is prohibited and may result in disciplinary action.

Sanctions

Breaches of this policy may result in:

- Temporary or permanent withdrawal of ICT access;
- Withdrawal of internet access;
- Internal disciplinary sanctions;
- Suspension or exclusion;
- Referral to external agencies, including the police, where appropriate.

All sanctions will be proportionate, reasonable and consistent with the Behaviour Policy, Safeguarding and Child Protection Policy, and associated College procedures.