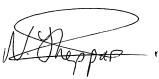




Online Safety Policy

2026/2027

Author:	Natalie Bracegirdle
Approved By:	Academy Committee
Signature:	
Approval Date:	September 2026
Review Frequency:	Annual, or sooner where legislation, guidance, technology or risk changes
Next Review:	September 2027
Applies to:	All students, staff, governors, volunteers, contractors, visitors and other users of school technology

1. Purpose and status

Online safety is an integral part of safeguarding at Carisbrooke College. This policy sets out the school-level arrangements for preventing, identifying and responding to online safety risks. It should be read alongside the HISP Safeguarding and Child Protection Policy and Procedures and the Trust and school policies listed in section 17. It does not replace the safeguarding procedures in the HISP policy.

2. Aims

- Protect pupils, staff, volunteers and governors from harm associated with the use of digital technology.
- Promote confident, safe, responsible and respectful use of technology.
- Ensure online safeguarding is embedded in curriculum, pastoral work, staff practice and wider school culture.
- Provide clear routes for reporting, recording, responding to and escalating online safety concerns.
- Maintain effective filtering and monitoring arrangements and ensure their effectiveness is reviewed at least annually.
- Provide governors with appropriate assurance and challenge regarding online safety, filtering and monitoring.

3. Scope

This policy applies to all members of the Carisbrooke College community and covers school-owned or school-managed devices, networks, accounts and services, as well as online activity connected to the school where it may affect the safeguarding, welfare, behaviour or reputation of pupils or staff. Concerns arising outside school will be managed in accordance with the HISP safeguarding, behaviour and other relevant procedures where the school has a safeguarding or disciplinary responsibility.

4. Principles

- Online safety is a safeguarding responsibility, not solely a technical responsibility.
- Children can be harmed online and offline; the same safeguarding principles apply in both contexts.
- The school will listen to pupils, take concerns seriously and act proportionately.
- Technology should support learning and inclusion while risks are actively assessed and managed.
- No filtering or monitoring system can guarantee complete protection; human oversight, education and safeguarding response remain essential.
- Staff must model professional and responsible digital behaviour.

5. Online risks

Carisbrooke College adopts the HISP four-category framework:

Content: Exposure to illegal, inappropriate or harmful material, including pornography, racism, misogyny, self-harm, suicide, antisemitism, radicalisation, extremism, misinformation, disinformation and conspiracy theories.

Contact: Harmful interaction with others, including peer pressure, grooming, exploitation, adults posing as children, commercial contact and other inappropriate online relationships.

Conduct: Behaviour that causes or increases the likelihood of harm, including cyberbullying, sharing explicit material, sharing nudes or semi-nudes, harassment and harmful online behaviour.

Commerce: Online gambling, inappropriate advertising, phishing, scams, financial exploitation and other risks involving money or commercial activity.

6. Responsibilities

6.1 Governors / Academy Committee

- Provide strategic oversight and challenge regarding online safety as part of safeguarding.
- Receive assurance that appropriate filtering and monitoring systems are in place and that their effectiveness is reviewed at least annually.
- Ensure governors receive safeguarding and online safety training and understand their responsibilities.
- Scrutinise relevant safeguarding, filtering/monitoring and online incident information without accessing unnecessary personal data.
- Approve or recommend approval of this policy in accordance with HISP governance arrangements.

6.2 Headteacher and Senior Leadership Team

- Ensure this policy is implemented and reviewed.
- Ensure online safety is integrated into safeguarding, behaviour, curriculum and staff development.
- Work with the DSL and IT support to identify risks and respond to incidents.
- Ensure appropriate action is taken when online activity presents a safeguarding or behavioural concern.

6.3 Designated Safeguarding Lead

- Lead the safeguarding response to online safety concerns.
- Ensure concerns identified through filtering, monitoring, staff reports or pupil disclosures are considered through safeguarding procedures.
- Work with IT/technical colleagues to understand filtering and monitoring alerts and reports.
- Ensure online safety forms part of safeguarding training, risk assessment and assurance.
- Escalate concerns to external agencies where required by the HISP safeguarding procedures.

6.4 IT / technical support

- Maintain filtering, monitoring, network and security arrangements in line with HISP requirements and the DfE Digital and Technology Standards.
- Provide appropriate reports and alerts to designated safeguarding and leadership colleagues.
- Record relevant checks, changes, incidents and actions.
- Work with the DSL and SLT on annual review, risk assessment and testing.
- Ensure new devices and services are appropriately configured before use.

6.5 Staff and volunteers

- Use technology professionally and in accordance with the Staff Code of Conduct and Acceptable Use arrangements.
- Use approved school systems for professional communication with pupils wherever possible.
- Report online safety or safeguarding concerns promptly through the school's safeguarding procedures.
- Model respectful, safe and responsible online behaviour.
- Maintain appropriate professional boundaries and protect personal information.

6.6 Pupils

- Use school technology and accounts responsibly and in accordance with the Acceptable Use arrangements.

- Treat others respectfully online and offline.
- Report harmful, unsafe, bullying, exploitative or inappropriate online activity.
- Protect passwords and personal information and avoid deliberately bypassing school security or filtering.

6.7 Parents and carers

- Support the school's expectations for safe and responsible technology use.
- Raise concerns promptly with the school where online activity may affect a child's safety or wellbeing.
- Use school communications and guidance to understand current arrangements for mobile phones, devices and online safety.

7. Education and prevention

Online safety will be taught through the curriculum and reinforced through pastoral provision, assemblies, RSHE and other appropriate opportunities. Teaching will include safe use of social media and technology, privacy and personal information, respectful online behaviour, recognising unacceptable behaviour, cyberbullying, online exploitation, radicalisation and other age-appropriate risks. Pupils will be encouraged to report concerns, including concerns affecting other pupils.

Parents and carers will be provided with age-appropriate online safety information through school communications, the website and other appropriate engagement opportunities.

8. Filtering and monitoring

Carisbrooke College will maintain robust filtering and monitoring arrangements appropriate to the age, context and risk profile of the school. Filtering is a preventative control; monitoring is a reactive safeguarding control. Both require appropriate human oversight.

- The DSL will lead on safeguarding implications and receive relevant reports/alerts.
- IT support will maintain technical systems and provide reports, alerts and evidence of checks.
- Filtering and monitoring will cover relevant school-managed internet-connected devices and services, including where devices are used off-site.
- The school will ensure staff know how to report and record concerns arising from filtering or monitoring.
- Checks will be recorded, including the date, person responsible, what was tested and any resulting action.
- The effectiveness of filtering and monitoring will be reviewed at least annually by SLT, the DSL and IT support, with involvement from the responsible governor/Academy Committee.
- The annual review will consider the school's risk profile, changes in technology, new services including AI, emerging safeguarding risks and any incidents or weaknesses identified.
- Monitoring information will be handled securely and only accessed by authorised staff with a legitimate need.

9. Mobile phones and smart technology

Carisbrooke College operates a school mobile phone procedure. From 29 June 2026, the school introduced revised arrangements for mobile phones, and the school subsequently reported the use of QuietCases as part of its approach. The detailed operational procedure is maintained separately so it can be updated without requiring this safeguarding policy to be rewritten.

The school's mobile phone arrangements will be implemented consistently with the DfE statutory guidance on mobile phones in schools and the HISP safeguarding framework. Staff may search or confiscate pupil devices only in accordance with applicable law and the school's published procedures.

10. Digital communications, images and professional boundaries

- Staff must use approved school systems and professional accounts for communication with pupils.
- Communication with pupils must be professional, transparent and capable of appropriate scrutiny.
- Staff must not use personal social media accounts to establish inappropriate relationships with pupils.
- Digital photographs, videos and other pupil information must be handled in accordance with school procedures, data protection requirements and relevant consent/permission arrangements.
- Personal data must not be shared through unapproved services or accounts.

11. Artificial intelligence

Carisbrooke College recognises that generative AI can support teaching, learning and safeguarding but may also create risks including harmful content, bullying, grooming, misinformation, privacy risks and deepfakes. New AI tools used by the school will be subject to appropriate risk assessment before implementation. Any harmful or abusive use of AI will be managed through the safeguarding, behaviour, acceptable use and other applicable procedures.

12. Responding to incidents and concerns

Any person who becomes concerned about a pupil's safety online should report the concern promptly through the school's safeguarding procedures. A member of staff must not investigate a potential safeguarding matter beyond what is necessary to establish and report the concern, and must not promise confidentiality.

- Safeguarding concerns must be referred to the DSL/DDSL in accordance with the HISP Safeguarding and Child Protection Policy.
- Concerns may include cyberbullying, grooming, exploitation, radicalisation, harmful sexual behaviour, sharing of nudes/semi-nudes, exposure to harmful content, threats, coercion, scams or other online harm.
- Where there is immediate danger or a concern of significant harm, the HISP safeguarding procedures and relevant emergency/referral arrangements must be followed.
- Online incidents may also require action under the Behaviour, Anti-Bullying, Staff Code of Conduct, Acceptable Use or disciplinary procedures.
- Relevant incidents and decisions will be recorded in accordance with HISP safeguarding and records-management requirements.

13. Training and awareness

All staff will receive safeguarding training that includes online safety and the expectations, roles and responsibilities around filtering and monitoring. Online safety will be reinforced through regular safeguarding updates. Governors will receive safeguarding and online safety training appropriate to their role.

14. Equality, inclusion and additional vulnerability

The school recognises that some pupils may face increased online risk or additional barriers to recognising, reporting or disclosing harm. Online safety education, risk assessment and safeguarding responses will take account of individual needs, including SEND, language, vulnerability, exploitation risk and other relevant contextual factors.

15. Monitoring, assurance and reporting to governors

The DSL and senior leaders will provide appropriate assurance to governors through the school's safeguarding monitoring arrangements. This may include, as appropriate and without unnecessary disclosure of personal information:

- The outcome of the annual filtering and monitoring review.
- Evidence that relevant checks have been completed and actions followed up.
- Themes and trends from online safety incidents and safeguarding concerns.
- Staff training and awareness activity.
- Curriculum and pupil voice information relating to online safety.
- Key changes in technology, emerging risks and any resulting risk-control measures.
- Progress against actions arising from safeguarding reviews, audits or inspections.

16. Policy review

This policy will be reviewed annually and sooner where required by changes to legislation, statutory guidance, HISP policy, technology, school practice or the school's assessed risk profile. The review will be informed by the annual online safety risk assessment and filtering/monitoring review.

17. Related policies and guidance

- [HISP Safeguarding and Child Protection Policy and Procedures](#)
- [Mobile Phone Use procedure](#)
- [HISP Staff Code of Conduct](#)
- [Behaviour and Culture Policy](#)
- [Anti-Bullying Policy](#)
- [Data Protection](#)
- [Cyber Security](#)
- RSHE and Curriculum policies
- Searching, Screening and Confiscation guidance
- Keeping Children Safe in Education 2026 (in force from 1 September 2026)
- DfE Filtering and Monitoring: Core Standard
- DfE Mobile Phones in Schools guidance
- [AI Policy](#)

Appendix 1 – Changes from the 2023 IWEF E-Safety Policy

Area	Change
Governance	Moves from the former IWEF E-Safety Governor/Coordinator structure to the HISP safeguarding and school governance framework.
Safeguarding	Makes explicit that online safety is part of the HISP safeguarding framework rather than a standalone technical issue.
Terminology	Uses 'Online Safety' rather than 'E-Safety'.
Current risks	Adds clearer coverage of misinformation, disinformation, conspiracy theories, online exploitation, commerce-related harms and AI/deepfakes.
Filtering and monitoring	Strengthens the annual review, risk assessment, recorded checks and governor assurance requirements.
Mobile phones	Reflects current Carisbrooke arrangements and the 2026 DfE statutory mobile-phone guidance.
Training	Aligns online safety training with HISP's wider safeguarding training and annual expectations.
Data protection	Avoids duplicating data protection law and procedures now covered by separate Trust/school arrangements.
Incident response	Directs safeguarding incidents into the HISP safeguarding procedures rather than maintaining a separate legacy online-safety incident flowchart.
Document structure	Removes duplicated material from the 2023 IWEF policy and concentrates this document on Carisbrooke's local implementation and governance assurance.

Appendix 2 – Governor approval and annual assurance checklist

- ☐ Policy reviewed against current HISP safeguarding arrangements.
- ☐ Annual filtering and monitoring review completed and recorded.
- ☐ Online safety risk assessment completed/reviewed.
- ☐ Staff online safety training/update completed.
- ☐ Governor safeguarding/online safety training up to date.
- ☐ Mobile phone arrangements reviewed against current DfE requirements.
- ☐ Online incident themes and safeguarding trends reviewed.
- ☐ Actions from audits/reviews assigned and monitored.