Online Safety Policy

May 2026

(Version 2)

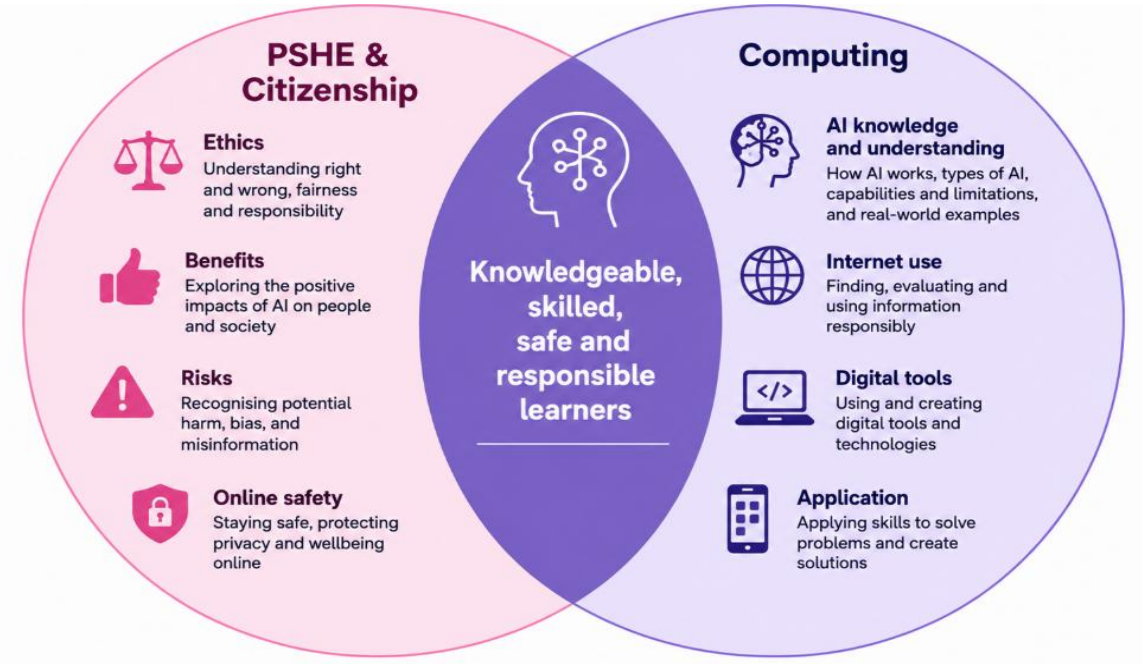
The Online Safety Policy has been discussed and adopted by the Local Advisory Board in May 2026	
Chair of Local Advisory Board:	*Mr G Provis*
Responsible Officer:	*Mrs C Sleath*
Agreed and ratified by the Local Advisory Board on:	*June 2026*
To be reviewed:	*June 2027*

Complementary Policies

Within the CFLP, the Online Safety, Computing and PSHE & Citizenship work in complementary alignment to ensure pupils develop both the *knowledge* and the *judgement* required to engage safely in modern digital life.

- Computing equips pupils with the technical skills and knowledge including how to effectively navigate the internet and elements of A.I.
- PSHE & Citizenship provides the ethical framework, enabling pupils to understand the benefits, risks and responsible use of online environments and A.I. including safety, wellbeing and digital citizenship.
- The overlap between the two disciplines is critical, ensuring that pupils can apply their technical understanding safely, responsibly and effectively.

Together, these areas ensure that pupils are not only digitally competent but also digitally responsible, aligning with best practice in safeguarding and online safety education (e.g. DfE *Teaching Online Safety in Schools*, Education for a Connected World framework).



Introduction

The Children First Learning Partnership (CFLP) is committed to ensuring that all learners and staff are safe, responsible and empowered users of digital technologies across all trust schools. The CFLP vision recognises the uniqueness of every child, champions inclusion, promotes aspiration, inspires learning, and encourages all learners to become responsible citizens of the future. These values underpin our approach to digital safety,

ensuring that all schools create environments where learners understand both the opportunities and risks associated with technology.

This policy aims to:

- Ensure every learner becomes a safe, respectful and responsible digital citizen.
- Provide clarity for staff, governors, pupils and parents on safeguarding expectations.
- Support schools in implementing consistent online safety practice across the Trust.
- Embed online safety in all areas of curriculum and school life.

Curriculum Intent and Digital Citizenship

The CFLP ensures that online safety is woven into the wider curriculum intent, recognising the need for a progressive, knowledge-rich and contextually relevant education. Beginning in EYFS, pupils learn how to explore technology safely. As they progress, they are introduced to concepts such as the SMART rules, recognition of trustworthy information, respectful communication, privacy awareness and safe online identity behaviours.

At the CFLP, digital citizenship includes:

- Understanding online rights and responsibilities.
- Evaluating the reliability and credibility of online content.
- Respecting intellectual property, including copyright and plagiarism awareness.
- Demonstrating empathy, kindness and respect in online interactions.
- Understanding digital footprints and long-term online reputation.

Through Computing, PSHE & Citizenship, English, and cross-curricular digital experiences, pupils learn how to navigate online environments safely and effectively. Learning objectives are mapped across the CFLP PSHE & Citizenship (3D PSHE scheme) and Computing Progression documents to ensure coherence and age-appropriate sequencing across all phases.

Our online safety provision is structured around the recognised strands from the *Education for a Connected World* framework. Pupils revisit and build upon key themes each year:

- Self-image and Identity
- Online Relationships and Reputation
- Online Bullying
- Health, Wellbeing and Lifestyle
- Managing Online Information
- Copyright and Ownership
- Privacy and Security

Through these themes, children learn how to develop positive online relationships, recognise and respond to risks, manage their digital footprint, and understand how to use technology safely, respectfully and responsibly.

This progressive approach supports statutory requirements for Relationships and Health Education 2026 and complements the Computing curriculum.

The 5Cs Model of Online Safety

The Trust adopts the updated 5Cs model of online risk, which builds on the traditional 4Cs and reflects the addition of "Credibility" in the 2025 KCSIE update. Each category is explicitly taught and reinforced across the curriculum:

1. **Content** – Exposure to harmful or inappropriate material, including extremist content, pornography, violence, self-harm or hate.

2. **Contact** – Risks of harmful or manipulative interactions such as grooming, coercion, unwanted communication or contact via gaming, messaging apps or social networks.

3. **Conduct** – Behaviours that can harm oneself or others, including cyberbullying, aggression, sharing inappropriate images, hacking attempts, or online rule-breaking.

4. **Commerce** – Commercial exploitation such as scams, gambling, phishing, fraudulent messaging and online financial targeting.

5. **Credibility** – Misinformation, disinformation, conspiracy theories, online fakeness (including deepfakes), deceptive AI-generated content, and misrepresentation.

Pupils are taught to critically evaluate online information, understand how algorithms and persuasive design influence behaviour, and recognise when information may be misleading or manipulated.

Implementation across CFLP Schools

Implementation strategies reflect the developmental stages of pupils and ensure consistent trust-wide practice:

EYFS:

- Early exposure to safe technology use.
- Recognising trusted adults and knowing when to ask for help.
- Beginning awareness of personal information and privacy.

Key Stage 1:

- SAFE online behaviours through the SMART rules.
- Understanding private vs. public information.
- Recognising upsetting or confusing content and seeking help.
- Introduction to digital citizenship and respectful communication.
- Introduction to AI-generated content, bias and misinformation.

Key Stage 2:

- Safe use of email, search engines and collaborative tools.
- Identifying cyberbullying and understanding consequences.
- Understanding copyright, ownership and plagiarism.
- Developing research skills and evaluating credibility of content.
- Explore AI-generated content, bias and misinformation.

Progression is monitored through Evidence Me, classwork and teacher assessments. Online safety is embedded not only through Computing but across PSHE & Citizenship, English, Humanities, assemblies, themed weeks and national events such as Safer Internet Day.

Roles and Responsibilities

Online safety is a shared responsibility across the Trust:

Learners:

- Follow pupil Acceptable Use Agreements.
- Report concerns about unsafe or inappropriate content.
- Demonstrate responsible behaviour both in school and at home.
- Respect others online and contribute positively.

Staff:

- Act as role models in digital conduct.
- Maintain a zero-tolerance approach to cyberbullying and discrimination.
- Embed online safety naturally throughout teaching.
- Supervise digital device use and ensure age-appropriate filtering.

DSLs and Online Safety Leads:

- Maintain oversight of all online safety concerns.
- Deliver staff training and ensure KCSIE compliance.
- Oversee filtering, monitoring, incident logging and safeguarding responses.

Trust Board and Local Governing Committees:

- Monitor implementation and impact across all schools.
- Ensure all safeguarding requirements are met.
- Review policies annually or in response to incidents.

Parents/Carers:

- Support children in safe online use at home.
- Engage with Trust guidance, newsletters and workshops.

Integration with PSHE & Citizenship and Safeguarding

Online safety is fully embedded within PSHE & Citizenship, safeguarding teaching, and pastoral systems. Pupils explore topics such as consent, respectful relationships, resilience, emotional wellbeing, digital footprints, peer influence, social pressures, and managing online conflict.

Safeguarding teams monitor online safety issues through behaviour logs, monitoring alerts and filtering systems. Themes emerging in safeguarding data inform future curriculum planning and targeted interventions, including via class assemblies, circle times, adaptation to the planned PSHE & Citizenship curriculum

Assessment and Impact Measures

Impact is assessed through:

- Pupil voice discussions on safety, online behaviour and digital confidence.
- Evidence Me portfolios showcasing online safety understanding.
- Monitoring of incidents, reports and safeguarding logs.
- Teacher assessments during Computing and PSHE & Citizenship lessons.
- Analysis of filtering/monitoring reports.

The expectation is that by Year 6, pupils can critically analyse online environments, make safe decisions, recognise misinformation and manage online interactions responsibly.

Filtering, Monitoring and Technical Systems

The CFLP adheres to DfE Technical Standards for filtering and monitoring. All schools use robust, age-appropriate filtering to block harmful content and monitoring systems to detect concerning behaviours or risks. The DSL, Online Safety Lead, IT provider, and senior leaders conduct monthly checks of filtering arrangements. Alerts are investigated promptly, and actions recorded.

Filtering and monitoring systems cover:

- ✓ Attempts to access harmful content.
- ✓ Searches relating to self-harm, extremism or violence.
- ✓ Concerning communications.
- ✓ Use of unapproved apps or bypass tools.

Online Behaviour and Incident Reporting

All incidents of online harm follow CFLP safeguarding procedures. Pupils are taught how to report concerns using the SMART "Tell" rule and classroom systems. Staff log concerns on our safeguarding platform (My Concern) for DSL review. Serious incidents (e.g., grooming, illegal imagery, threats, extremism) are escalated to external agencies including the police.

Restorative, educational and disciplinary responses are used where appropriate to address harmful online behaviour.

A.I., Misinformation and Digital Literacy

The CFLP recognises A.I. as a rapidly developing technology with significant educational potential and safeguarding risks. Pupils are taught to:

- Understand how AI systems work at a basic level.
- Recognise bias or unfair outputs.
- Avoid sharing personal information with A.I. systems.
- Question the authenticity of images, videos and information.
- Identify deepfake content and understand how misinformation spreads.

Staff only use Trust-approved A.I. tools, never entering personal, sensitive or confidential data. All A.I.-assisted content must be reviewed for accuracy and appropriateness.

Community Engagement

The CFLP engages parents and carers through workshops, newsletters, online safety updates and resources. Families receive guidance on safe device use, privacy settings, social media use, cyberbullying prevention, and supporting children as they navigate digital spaces. Partnerships with external agencies strengthen the Trust's online safety network.

Review and Governance

The policy is reviewed annually by the Trust Board, DSL network and Online Safety Leads or earlier in response to emerging risks, serious incidents, or updates in statutory guidance. Schools provide monitoring data to the Trust to support ongoing evaluation. Continuous improvement ensures that CFLP remains proactive and effective in safeguarding the digital lives of all pupils.