

# Policy

## CPS02

<b>TITLE OF POLICY</b>	Digital and Online Safety
<b>FIRST RELEASE DATE</b>	
<b>LAST RATIFIED DATE</b>	Term 3 2025
<b>DATE FOR NEXT REVIEW</b>	Term 3 2026
<b>OWNER</b>	Michael Torrington
<b>REVIEWER</b>	Kathryn Honey



### Digital and Online Safety

#### 1. Aim

We recognise the importance of technology in education and take a proactive approach to safeguarding the community in the digital world. With the rapid changes in devices, tools, and platforms, educating our community about safe online behaviour is as crucial as ensuring safety in other areas of life. This policy ensures that staff, students, and parents can safely use digital technologies, including generative AI and the internet, to enhance learning and productivity, while maintaining the security of the school's digital infrastructure. We are committed to safeguarding the school's digital assets and personal data, ensuring compliance with legal standards, and fostering a culture of cybersecurity.

#### 2. Scope

Online behaviour must align with the same transparency, privacy, and respect standards as offline interactions. Online activities are permanent, and by using the ICS network, users agree to monitorable, public actions. This policy ensures safe technology use, protects against harmful content, promotes responsible use, and safeguards the school's systems from security breaches. It also establishes responsibilities for staying safe online and responding to cyber threats, protecting both the infrastructure and sensitive information.

#### Staff Acceptable Use

All technology resources are for educational purposes only. Personal use, entertainment, and accessing inappropriate content are prohibited. The responsible use of generative AI must align with educational goals. Harassment, bullying, or intimidation via technology is not tolerated. All students must be safeguarded during online activities. Staff must protect their login credentials, report breaches promptly, and comply with ongoing professional development, including achieving Google Educator Level 1 certification within the first year. Technology use is monitored, and violations may result in disciplinary actions.

#### Student Acceptable Use

Students are responsible for keeping their login details secure and for using school systems, devices, and communications only for educational purposes. Personal interactions, private information sharing, and online engagement with strangers are prohibited. Students must avoid gaming, file sharing, or video streaming without explicit permission. Any inappropriate content should be reported immediately. Respect for others' work and property and adhering to digital citizenship guidelines

are required. Violations may result in disciplinary actions, including losing access to systems and communication with parents.

### Online Safety

To maintain safety online:

- Use ICS Google Workspace logins for learning activities.
- Keep login details private and respect others' personal information.
- Trust your instincts and report uncomfortable situations immediately.
- Do not engage in cyberbullying, and report it when it is observed.
- Use only trusted, vetted websites and resources.
- Communicate respectfully, be mindful of your digital footprint, and practice responsible media literacy.

### Online Learning Attitudes

Demonstrate responsible, ethical technology use, communicate thoughtfully, be patient and understanding with others, and maintain a willingness to learn and adapt to new tools and platforms.

### Responding to a Data Breach

- IT will shut down affected systems and notify relevant parties.
- Report breaches and change passwords immediately.
- IT will assess the situation and document the incident.

## 3. Unique Definitions

**E-Safety:** refers to the practices and strategies used to ensure safety while engaging in online activities.

**Digital Citizenship:** the responsibility to act safely and ethically online.

**Media Literacy:** the ability to critically evaluate, create, and share media content, including understanding its credibility, biases, and the motives behind its production.

**Digital Footprint:** all online interactions, such as browsing history, shared data, and location tracking.

**Cyberbullying:** the use of digital tools, such as emails or social media, to harass or intimidate others.

**Identity Fraud:** occurs when someone steals another person's login credentials to impersonate them online.

**Ransomware:** malicious software that encrypts data and demands payment for decryption, often spread through deceptive emails.

**Phishing:** a deceptive practice where attackers impersonate legitimate entities to steal sensitive information, typically via email.

**Data Leakage:** occurs when sensitive information is exposed or accessed without authorisation.

**Hacking:** refers to unauthorised access to IT systems, often through deceptive methods like social engineering, to obtain sensitive data.

**Generative AI:** artificial intelligence systems designed to create new content, such as text, images, or audio, based on input data.

**Data Protection:** refers to the practices and regulations used to ensure that personal information is stored securely and handled responsibly to prevent unauthorised access.

**Encryption:** the process of converting data into a secure format that can only be read or decoded by authorised users or systems.

**Two-Factor Authentication (2FA):** a security process in which users must provide two forms of verification before gaining access to an account, typically a password and a one-time code sent to a mobile device.

**Malware:** software specifically designed to disrupt, damage, or gain unauthorised access to computer systems, including viruses, worms, and spyware.

**Spam:** refers to unsolicited or irrelevant messages, typically sent via email, often for commercial or malicious purposes.

#### 4. Associated Forms and Documents

[Staff Technology Acceptable Use Agreement](#)

 Student Acceptable Use Agreement- Y1-3

 Student Acceptable Use Agreement- Y4-6

 Student Acceptable Use Agreement- Y7-13

#### 5. Related Information

# Policy

## CPS02

[Google Privacy & Terms 31st March 2024](#)

[Privacy and Electronic Communication Regulations 2019](#)

[The Data Protection Act 2018](#)

[The Copyright Designs and Patents Act 1988](#)

[The Computer Misuse Act 1990](#)

[A framework for Digital Citizenship Implementation \(Common Sense Education\)](#)

[Keeping Children Safe in Education 2025](#)

[Working Together to Safeguard Children](#)