



Inspire, Enjoy, Achieve

E-Safety Policy

February 2016

Reviewed March 21

Reviewed September 2025

Reviewed September 2026

Review September 2027

Cotton End Forest School

E-Safety Policy

Rationale

At Cotton End Forest School, we recognise the importance of teaching children how to use technology safely, respectfully and responsibly. As digital tools become increasingly embedded in education and daily life, it is vital that pupils understand how to protect themselves and others online. High-quality e-safety education supports safeguarding, promotes wellbeing and empowers children to make informed choices.

Aims

- To safeguard pupils when using digital technologies in school and at home
- To educate pupils about responsible online behaviour, cyberbullying and digital footprints
- To ensure staff and parents are informed and confident in supporting children's online safety
- To establish clear procedures for reporting and responding to e-safety concerns
- To promote safe use of educational platforms such as **Purple Mash**
- To ensure sensitive data is handled securely and in line with data protection regulations

Roles and Responsibilities

Senior Leadership Team (SLT)

- Embed e-safety into safeguarding and curriculum policies
- Monitor and review the effectiveness of e-safety practices
- Support staff with training and resources

Designated Safeguarding Lead (DSL)

- Lead on e-safety incidents and concerns
- Liaise with external agencies where necessary
- Maintain records of e-safety breaches and actions taken

Teachers and Support Staff

- Model safe and responsible use of technology
- Deliver e-safety lessons and respond to pupil concerns
- Monitor pupil use of platforms such as **Purple Mash**
- Report any e-safety incidents to the DSL

Pupils

- Follow the school's Acceptable Use Agreement

- Use technology respectfully and responsibly
- Use **Purple Mash** and other platforms only for learning purposes
- Report anything that makes them feel uncomfortable or unsafe

Parents and Carers

- Support the school's e-safety approach
- Monitor their child's online activity at home
- Engage with school communications and guidance on e-safety

Curriculum and Teaching

E-safety is taught explicitly through Computing and PSHE lessons, and reinforced across the curriculum. Pupils learn about:

- Keeping personal information private
- Recognising and reporting inappropriate content or contact
- Understanding cyberbullying and how to respond
- Evaluating online sources and avoiding misinformation
- The impact of digital footprints and online reputation
- Safe and responsible use of **Purple Mash**, including messaging, blogging and file sharing features

We use age-appropriate resources such as **ThinkUKnow**, **Childnet**, **BBC Own It** and **Purple Mash's e-safety modules** to support learning.

Technology and Filtering

- The school uses secure filtering and monitoring systems to restrict access to inappropriate content
- All devices are protected with antivirus and security software
- Pupils use school devices under adult supervision
- Staff devices are password-protected and regularly updated
- The school uses **Classroom Cloud** to monitor pupil activity on devices in real time, helping staff guide safe and focused use of technology during lessons
- **Purple Mash** is monitored by staff to ensure safe use of its interactive features

Data Protection and Secure Use of Digital Platforms

At Cotton End Forest School, we are committed to protecting sensitive data and ensuring that all digital platforms used by staff and pupils are secure and compliant with data protection regulations.

Staff Use of Google Drive

- Staff may use **Google Drive** to access and store school-related documents remotely

- Files containing **personal or sensitive data** (e.g. pupil names, medical information, safeguarding records) must be stored in **secure, access-controlled folders**
- Staff must ensure their **Google accounts are password-protected** and are not shared with others
- Devices used to access Google Drive must be **locked when unattended**, and have up-to-date antivirus and security software installed
- Sensitive data must **not be downloaded to personal devices** unless absolutely necessary, and must be deleted promptly after use
- Staff must avoid using public Wi-Fi when accessing sensitive documents unless connected via a secure VPN

General Data Protection Guidelines

- All staff must follow the school's **Data Protection Policy** and **GDPR guidelines**
- Personal data must only be shared on a **need-to-know basis** and through secure channels
- Any data breach or suspected breach must be reported immediately to the **Data Protection Officer (DPO)** or DSL

Procedures for E-Safety Breaches

In the event of an e-safety breach - whether involving inappropriate content, cyberbullying, misuse of school systems, or unsafe online behaviour - the following steps must be taken:

1. Immediate Action

- Report the incident immediately to the **DSL** or a member of the **SLT**
- Secure and isolate any device involved to preserve evidence
- Ensure the safety and wellbeing of pupils involved

2. Recording the Incident

- Log the incident using the school's safeguarding or behaviour system
- Include date/time, individuals involved, nature of the breach, actions taken and follow-up required

3. Investigation

- The DSL will lead an investigation, reviewing digital activity and gathering relevant information
- If the breach involves **Purple Mash**, staff will review logs and user interactions

4. Parental Involvement

- Inform parents/carers promptly and appropriately
- Offer support and guidance to help manage any ongoing concerns

5. Follow-Up Actions

- Apply appropriate sanctions in line with the Behaviour Policy
- Provide additional education or support around safe online behaviour
- Refer to external agencies if necessary (e.g. CEOP, Police, Children's Services)

6. Review and Prevention

- Review the incident to identify gaps in policy, supervision or education
- Strengthen e-safety measures through updated filtering, staff training or curriculum changes

Communication and Engagement

- E-safety updates are shared with parents via newsletters, workshops and the school website
- Staff receive regular training and updates on emerging risks and best practices
- Pupils are encouraged to speak openly about their online experiences
- Guidance on safe use of **Purple Mash** is shared with families to support learning at home

Review

This policy will be reviewed annually by the SLT and Governing Body to ensure it remains current, effective, and responsive to emerging technologies and risks.