Hyde Park Schools

Online Safety Policy

Approved by: Executive Head Teacher **Date:** December 2025

Last reviewed: December 2025

Next Review Due: December 2026

1. Welcome & Our Shared Commitment

This isn't just a document; it's our promise to keep every child safe in the digital world, whether they are using a school tablet or logging in from home. This policy covers everyone in our community: staff, children, parents, governors, and visitors. Our core mission is simple: To ensure technology is used safely and brilliantly as a key part of our overarching responsibility to protect children (*KCSIE*).

1.1. Why This Matters Now

Our policy is built on the newest rules and best practices, including the principles of the Online Safety Act and the latest safeguarding guidance (*Keeping Children Safe in Education 2025*). We focus on being proactive, not just reactive.

1.2. Our Core Safety Recipe

We use the Four Cs of Online Risk to guide our teaching and systems. Our aim is to foster Digital Resilience—giving children the skills to cope and thrive when things get tricky online.

2. Who Does What? Our Safety Team

Keeping children safe is a team sport! Here's how the responsibilities are shared:

2.1. The Governors and Trustees (Our Oversight Guardians)

- **Approval & Checks:** They formally sign off on this policy and ask for termly updates to make sure our technology is meeting all the legal standards.
- **The E-Safety Governor:** One Governor is specially tasked with checking on our online safety practices and reporting back to the board.

2.2. School Leadership (The Navigators)

- **Training Champions:** They make sure all staff get comprehensive, mandatory training every year. This training includes new things like how to safely manage tools that use Artificial Intelligence (AI) and Machine Learning.
- **Setting the Rules:** They manage disciplinary issues, even if they happen outside of school, if they impact the school community (under the Education Act).

2.3. The E-Safety Lead (The Technical Expert)

This person works hand-in-hand with our IT team (HMAT/SWGfL) to manage the day-to-day tech side of safety.

- **Filter Control:** They make sure our filters are age-appropriate and that all school devices—even laptops taken home—are safely filtered.

- **Monitoring Alerts:** They are the first to check alerts generated by our monitoring systems (which watch for concerning searches like self-harm or grooming) and quickly pass serious concerns to the DSL.
- **Managing AI Risk:** They manage the controls on the school network regarding the use of new technologies, ensuring staff and children use online tools responsibly and don't try to access or create inappropriate content via systems like Generative AI chatbots.

2.4. Designated Safeguarding Lead (DSL) (The Safety Coordinator)

The DSL is the central point for managing child protection that comes from online activity.

- **Decision Maker:** They decide when a serious online incident needs to be referred to the Police, CEOP (Child Exploitation and Online Protection), or Social Services.
- **Understanding Vulnerability:** They are trained to see how online risks (like radicalisation or exploitation) affect children who are already vulnerable.

2.5. All Staff, Teachers, and Volunteers (The Role Models)

- **Know the Rules:** Everyone must sign our Staff Acceptable Use Policy (AUP) annually.
- **Active Supervision:** We keep a close eye on children when they are using technology, ensuring screens are visible.
- **Professional Contact is Key:** Staff must never use personal social media or private accounts to communicate directly with pupils. All contact must be professional and through official school channels.

3. Teaching Our Children to Be Smart Online

We don't just block things; we teach children to think critically and be confident online.

- **Learning Progression:** We use structured, fun resources (like CEOP's 'ThinkYouKnow') throughout the curriculum, especially in Computing and PSHE.
- **Critical Thinking:** We teach pupils:
    - How to check if a website is trustworthy before believing it.
    - That their digital footprint is permanent—what goes online stays online.
    - To be good digital citizens by respecting other people's work (copyright).
- **Infant School Focus (KS1):** For our youngest pupils, the focus is on safe contact, asking for help, and knowing the "tell" rule—telling a trusted adult if something feels wrong.

4. How We Keep the Gates Locked: Filtering and Monitoring

We have a legal duty to make sure our technical security is robust.

4.1. Filtering (The Digital Gatekeeper)

- Our system blocks all illegal content and anything inappropriate for an Infant school (e.g., adult content, self-harm instructions).
- This filtering covers all school devices and any personal devices connected to the school Wi-Fi.

4.2. Monitoring (The Early Warning System)

- **The Goal:** Our system watches for unacceptable behaviour or searches (e.g., terms related to self-harm, extreme content, or inappropriate contact attempts) and sends alerts to the E-Safety Lead.
- **Privacy Reminder:** Users are always told that monitoring takes place. The logs are only ever used for safeguarding and educational purposes, strictly following data privacy laws (UK GDPR).

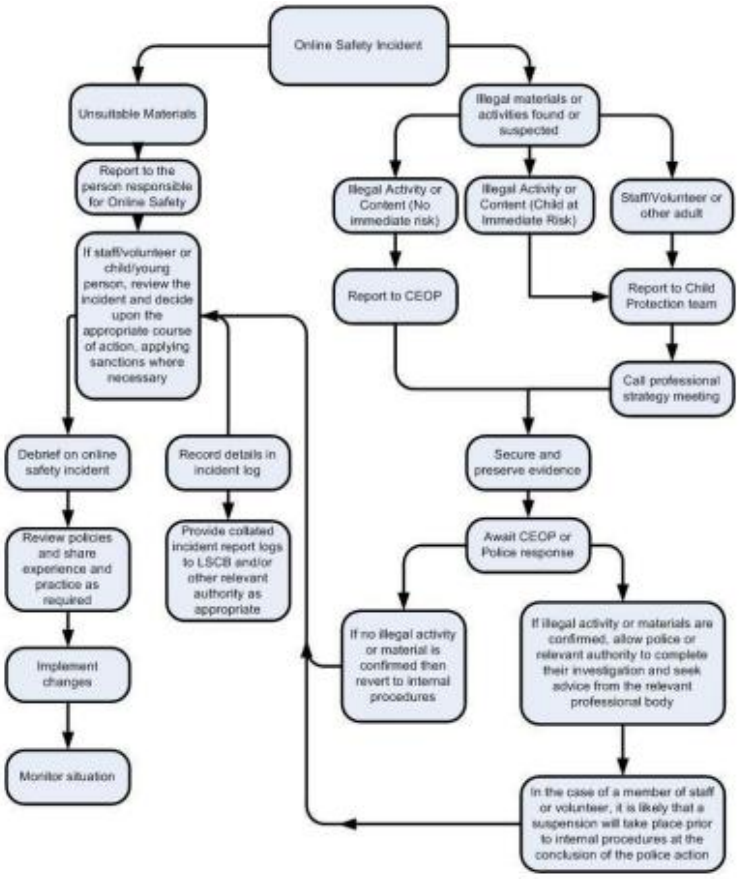
5. What to Do When Something Goes Wrong: Incident Protocol

When an incident occurs, we need a clear, rapid response.

5.1. Our Action Plan Flowchart

All staff must immediately consult the guidance outlined in the original policy document.

The following Flowchart is your guide for rapid response upon discovering an Online Safety Incident.



5.2. Quick Steps for Critical Incidents

1. **Safety First:** Check the emotional safety of the child(ren) involved.
2. **Securing Evidence** (Crucial): If you find something illegal (e.g., an illegal image or communication): DO NOT turn the device off. Isolate the screen or device and call the DSL/Headteacher immediately. Do not try to copy, save, or download the material.
3. **Referral:** The DSL will decide on referring the case to the Police or CEOP/Social Services within one hour for high-risk incidents.
4. **Logging:** Every incident, big or small, must be carefully recorded in our central safeguarding system (CPOMS).
5. **Acceptable Use and Consequences:** We expect everyone to use technology responsibly. Breaking the rules means clear, proportionate consequences.

6.1. Pupil Sanctions

We follow the Consequences Table for Pupils, which ranges from:

- A chat with the Class Teacher
- A meeting with the Leadership Team and parents
- Temporary loss of internet access

Pupils	Actions								
Incidents:	Refer to class teacher / tutor	Refer to Leadership Team	Refer to Headteacher	Refer to Police	Refer to technical support staff for action re filtering / security etc	Inform parents / carers	Removal of network / internet access rights	Warning	Further sanction e.g. detention /
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).			✓	✓					
Unauthorised use of non-educational sites during lessons	✓								
Unauthorised use of mobile phone / digital camera / other handheld device	✓				✓				
Unauthorised use of social networking / instant messaging / personal email	✓								
Unauthorised downloading or uploading of files	✓								

Allowing others to access school network by sharing username and passwords		✓								
Attempting to access or accessing the school network, using another student's / pupil's account	✓									
Attempting to access or accessing the school network, using the account of a member of staff		✓	✓			✓				
Corrupting or destroying the data of other users	✓									
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature		✓								

Continued infringements of the above, following previous warnings or sanctions		✓								
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school		✓								
Using proxy sites or other means to subvert the school's filtering system		✓			✓					
Accidentally accessing offensive or pornographic material and failing to report the incident		✓	✓		✓	✓				
Deliberately accessing or trying to access offensive or pornographic material		✓	✓	✓			✓			
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act		✓								

6.2. Staff Professional Conduct

Immediate and serious action will be taken for breaches such as:

- Trying to bypass the filtering system.
- Using personal accounts to communicate with pupils.
- Careless handling of confidential pupil data.

Staff Actions

Incidents:	Refer to Leadership Team	Refer to ISP	Refer to Police	Refer to Technical Support Staff for action re filtering etc	Warning	Disciplinary action
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).	✓	✓	✓	✓		✓
Inappropriate personal use of the internet / social networking sites / instant messaging / personal email	✓				✓	
Unauthorised downloading or uploading of files	✓					
Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person's account	✓				✓	
Careless use of personal data eg holding or transferring data in an insecure manner	✓					
Deliberate actions to breach data protection or network security rules	✓	✓				
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software	✓	✓				✓
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature	✓	✓				✓
Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with pupils not connected to education	✓			✓		✓
Actions which could compromise the staff member's professional standing						
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school						
Using proxy sites or other means to subvert the school's filtering system						
Accidentally accessing offensive or pornographic material and failing to report the incident						
Deliberately accessing or trying to access offensive or pornographic material						
Breaching copyright or licensing regulations						
Continued infringements of the above, following previous warnings or sanctions						

Any serious misconduct will lead to the Trust's formal disciplinary process and may involve the Local Authority Designated Officer (LADO).