connecteducationtrust.org

CONNECT EDUCATION TRUST

Connect Online Safety

What To Do If Guidance

2026-2029

Safeguarding in the digital world is an integral part of the school's whole-safeguarding approach. Online risks are categorised across the **4 Cs**: **Content** (including AI deepfakes, pornography, and online misinformation), **Contact**, **Conduct**, and **Commerce**.

Our school's approach prioritises the safety and well-being of our community by aligning with the latest statutory guidance, including Keeping Children Safe in Education (KCSIE), relevant DfE standards, and NCSC guidelines. This brief aims to reinforce a proactive, compliant, and supportive online safety culture for all staff, governors, and trustees.

An inappropriate website is accessed <u>unintentionally</u> in school by a teacher or pupil.

- **Immediate Action:** Remain calm. Reassure the pupil that they are not in trouble to maintain a "no-blame" reporting culture. Do not draw attention to the screen or create an unnecessary display.
- **Safeguarding Action:** Log the incident on the school's safeguarding system for the DSL. The DSL will review the technical context and decide if parents need to be notified about the exposure.
- **Filtering Maintenance:** Inform the School IT Lead / Managed Service Provider (MSP) immediately.
- **Compliance Standard:** The IT team must check the incident against the **DfE Meeting Digital and Technology Standards in Schools and Colleges (specifically the Filtering and Monitoring Standards)** and the Plan Technology for Your School tool. The URL must be blocked immediately via the filtering provider (e.g., LGfL). A formal block request must be logged to fulfill the annual filtering and monitoring system review.

An inappropriate website is accessed <u>intentionally</u> by a pupil.

1. **Behavioral Action:** Refer to the Acceptable Use Policy (AUP) signed by the pupil and apply agreed sanctions. Notify the parents of the pupil.
2. **Technical Action:** Inform school technicians / LGfL to ensure the site is properly filtered.
3. **Safeguarding Context:** The DSL must assess whether the intentional access indicates a wider safeguarding risk (e.g., radicalisation, exploitation, grooming, or child-on-child abuse) and determine if an early help or statutory referral is required, rather than treating it purely as a behavioral issue.

An adult uses School IT equipment inappropriately.

Immediate Action: Do not view or investigate the misuse alone, and do not draw other colleagues in to witness the material. Report the misuse immediately to the Headteacher (or the DSL). If the allegation involves the Headteacher, report directly and immediately to the Chair of Governors and the Local Authority Designated Officer (LADO).

If the material is offensive/inappropriate but NOT illegal:

1. The Headteacher (or Chair of Governors/LADO if applicable) will ensure the device is secured and access is blocked.
2. Instigate an ICT equipment audit to ensure no student access lines are vulnerable, referencing NCSC guidance.
3. Take appropriate disciplinary action via Human Resources and inform the Trust Board/CEO.

In an extreme case where the material is suspected to be ILLEGAL (e.g., Child Sexual Abuse Material - CSAM):

- Do not interact with, investigate, move, log on, or log off the device.

- Secure the physical room to prevent anyone else from entering, and contact the local police / High-Tech Crime Unit immediately.
- Document only the time, location, and device ID without accessing the data, and await police arrival. Only move or handle the device if explicitly instructed to do so on the phone by law enforcement (e.g., to prevent imminent physical theft or destruction).

A bullying incident directed at a pupil occurs through email or mobile phone technology, either inside or outside of school time, including child-on-child abuse.

1. **Immediate Support:** Advise the pupil not to respond. Instruct them to stop communication and block the user.
2. **Evidence Preservation:** Strictly advise the pupil NOT to delete any messages, accounts, or media, as this evidence is vital for school or police investigation.
3. Guidance: Refer to the school's anti-bullying policy, PSHE, and Statutory Relationships Education, RSE and Health Education Guidance to apply sanctions and support. Notify parents of all pupils involved.
4. **Reporting Escalation:**
    - Inform the service/email provider. If malicious or threatening comments are hosted on an external site, request removal, referencing duties under the Online Safety Act 2023.
    - If the incident involves online sexual exploitation, sexual coercion, or grooming, immediately preserve screenshots and submit them to CEOP (www.ceop.gov.uk). Do not use CEOP for general, non-sexual cyberbullying incidents, which must be handled via internal behavior policies or local police contact.
    - Inform the Trust Board/CEO if comments target staff or heavily impact school reputation. Contact the police if criminal threats are made

You are concerned that a pupil's safety is at risk because you suspect someone is using communication technologies (such as social networking sites) to make inappropriate contact with the pupil

- **Immediate Action:** Report directly to the DSL. The school will coordinate a contact strategy with parents adhering strictly to KCSIE guidance.
- **Pupil Guidance:** Guide the pupil on how to safely cease contact and preserve evidence.
- **Exploitation Alert:** Be highly alert to signs of Financially Motivated Sexual Extortion (FMSE), where criminal networks coerce pupils into sharing intimate photos and subsequently blackmail them. If FMSE or grooming is suspected, report immediately to CEOP and the police.
- **Extremism Alert:** If online content or contact relates to radicalisation or extremism, the DSL will log this immediately in accordance with the Prevent Duty and contact external Channel/Prevent teams.

General Compliance

- Reporting Mandate: All the above incidents must be reported immediately to the Headteacher and the DSL as per Keeping Children Safe in Education (KCSIE) requirements.
- Culture: Pupils must be supported in a no-blame culture when reporting digital incidents so they can do so without fear of unnecessary punishment.
- Data Privacy: All handling of personal data during incident responses must comply with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 (DPA 2018).

Information

Because a cyber security breach directly threatens child safety, data protection is treated as a core safeguarding vulnerability.

- **Evidence Security:** All digital screenshots, metadata, and logs containing Personal Identifiable Information (PII) must be encrypted and stored solely within the school's restricted safeguarding system. Storing evidence on personal devices or unencrypted local drives is a severe policy breach.

- **Information Governance:** The school's **Data Protection Officer (DPO)** must be consulted on the deployment of all digital filtering, AI-risk tools, and monitoring software to ensure a Data Protection Impact Assessment (DPIA) is fully active

- If any personal data or evidence is shared with unauthorised parties or leaked during an incident response, it must be reported to the Data Protection Officer (DPO) immediately to assess if a self-report to the Information Commissioner's Office (ICO) is required within 72 hours.