connecteducationtrust.org

CONNECT EDUCATION TRUST

Online Safety

What do we do if? Guidance

This document outlines the essential procedures for all staff and pupils to follow when encountering online safety incidents. It serves as a rapid reference guide for managing situations such as inappropriate online content, cyberbullying, or concerns about pupil contact, ensuring prompt and effective responses.

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) 2024, The Online Safety Act 2023, and relevant DfE and NCSC standards. This brief aims to reinforce a proactive, compliant, and supportive online safety culture within our school.

An inappropriate website is accessed unintentionally in school by a teacher or pupil.

1. Play the situation down; don't make it into a drama.
2. Report to the Headteacher/DSL (Designated Safeguarding Lead) as per Keeping Children Safe in Education (KCSIE) 2024 guidelines, and decide whether to inform the parents of any pupils who viewed the site.
3. Inform the school technicians and ensure the site is filtered in compliance with DfE Filtering and Monitoring Standards for Schools and Colleges (LGfL).

An inappropriate website is accessed intentionally by a pupil.

1. Refer to the acceptable use guidance that was signed by the pupil and apply agreed sanctions.
2. Notify the parents of the pupil.
3. Inform the school technicians and ensure the site is filtered if need be.
4. Inform the LGFL if the filtering service is provided

An adult uses School IT equipment inappropriately.

1. Ensure you have a colleague with you, do not view the misuse alone.
2. Report the misuse immediately to the Headteacher/ DSL and ensure that there is no further access to the device, following procedures aligned with DfE Cyber Security Standards for Schools and College
3. If the material is offensive but not illegal, the Headteacher should then:
    - Remove the device to a secure place.
    - Instigate an audit of all ICT equipment by the schools ICT managed service providers to ensure there is no risk of pupils accessing inappropriate materials in the school, referencing guidance from the National Cyber Security Centre (NCSC).
    - Identify the precise details of the material.
    - Take appropriate disciplinary action (contact Human Resources).
    - Inform Trust Board/CEO of the incident.
    - In an extreme case where the material is of an illegal nature:

    Contact the local police or High Tech Crime Unit and follow their advice, referencing relevant guidance from the National Cyber Security Centre (NCSC).
    - If requested to, remove the device to a secure place and document what you have done.

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

1. Advise the pupil not to respond to the message.
2. Refer to relevant guidance, including online safety, anti-bullying and PHSE and the Statutory Relationships Education, Relationships and Sex Education (RSE) and Health Education Guidance and apply appropriate sanctions.
3. Secure and preserve any evidence.

4. Inform the sender's email service provider, and consider if the incident falls under the scope of the Online Safety Act 2023 for reporting to relevant online platforms.
5. Notify parents of the pupils involved.
6. Consider delivering a parent workshop for the school community,integrating themes from Statutory RSE and Health Education Guidance.
7. Inform the police if necessary.
8. Inform the Trust Board/CEO if malicious or threatening comments are posted on an Internet site about a pupil or member of staff.
9. Inform and request the comments be removed if the site is administered externally, referencing duties under the Online Safety Act 2023 where applicable
10. Send all the evidence to CEOP at ww.ceop.gov.uk/contact_us.html.
11. Endeavour to trace the origin and inform police as appropriate.

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

- Report to and discuss with the named DSL in school and school should contact parents, adhering to Keeping Children Safe in Education (KCSIE) 2024 guidance.

- Advise the pupil on how to terminate the communication and save all evidence.
- Contact CEOP http://www.ceop.gov.uk/
- Consider the involvement of police and social services.
- Inform Trust Board/CEO.
- Consider delivering a parent workshop for the school community.

If concerns arise regarding online content that may be related to radicalisation or extremism, these must be reported in accordance with the Prevent Duty (2023) to the DSL and relevant external agencies.

All the above incidences must be reported immediately to the Headteacher and online safety officer (DSL) as per Keeping Children Safe in Education (KCSIE) 2024 requirements.

Pupils should be confident in a no-blame culture when it comes to reporting inappropriate incidents involving the internet or mobile technology: they must be able to do this without fear**.**

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).