

# Online Safety

## What do we do if?



**ENFIELD**  
LEARNING TRUST  
BE INCLUDED

| Version and Date |          | Action/Notes    | Date Written      | Date to be Reviewed |
|------------------|----------|-----------------|-------------------|---------------------|
| 1.0              | 10.10.17 | Approved by SLT | Reviewed Sept '17 | 1 Year - 2018       |

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

1. Play the situation down; don't make it into a drama.
2. Report to the Headteacher/e- safety officer and decide whether to inform the, parents of any children who viewed the site.
3. Inform the school technicians and ensure the site is filtered (LGfL)

**An inappropriate website is accessed intentionally by a child.**

1. Refer to the acceptable use guidance that was signed by the child, and apply agreed sanctions.
2. Notify the parents of the child.
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 and ensure that there is no further access to the device.
3. If the material is offensive but not illegal, the head teacher should then:
4. Remove the device to a secure place.
5. 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.
6. Identify the precise details of the material.
7. Take appropriate disciplinary action (contact Personnel/Human Resources).
8. Inform The Local Governing Board of the incident.
9. In an extreme case where the material is of an illegal nature:
10. Contact the local police or High Tech Crime Unit and follow their advice.
11. If requested to, remove the device to a secure place and document what you have done.

**A bullying incident directed at a child occurs through email or mobile phone technology, either inside or outside of school time.**

1. Advise the child not to respond to the message.
2. Refer to relevant guidance including online safety, anti-bullying and PHSE and apply appropriate sanctions.
3. Secure and preserve any evidence.
4. Inform the sender's e-mail service provider.
5. Notify parents of the children involved.
6. Consider delivering a parent workshop for the school community.
7. Inform the police if necessary.
8. Inform the CEO if malicious or threatening comments are posted on an Internet site about a member of staff, or the Headteacher if it is about a pupil.
9. Inform and request the comments be removed if the site is administered externally.
10. Secure and preserve any evidence.
11. Send all the evidence to CEOP at [ww.ceop.gov.uk/contact\\_us.html](http://ww.ceop.gov.uk/contact_us.html).
12. Endeavour to trace the origin and inform police as appropriate.

13. Inform LGB for a pupil and Trust board for a member of staff.

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

1. Report to and discuss with the named child protection officer in school and contact parents.
2. Advise the child on how to terminate the communication and save all evidence.
3. Contact CEOP <http://www.ceop.gov.uk/>
4. Consider the involvement of police and social services.
5. Inform Trust Board/CEO.
6. Consider delivering a parent workshop for the school community.

All of the above incidences must be reported immediately to the Headteacher and online safety officer.

**Children 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.**

Signature of Chief Executive Officer: