
	Name of School	Corbets Tey School
	Guidance review Date	Autumn Term 2021
	Date of next Review	Autumn Term 2022
	Who reviewed this guidance?	Governor name: Phil Brimson Governor signature: 

Online Safety Guidance: What do we do if?

We have a Designated Safeguarding Lead (DSL) who has responsibility for Child Protection and Adult Safeguarding and who undertakes regular training for this role. This is the Headteacher, Mrs Emma Allen.

We have two Deputy Headteachers who will act as designated Safeguarding deputies in the Designated Safeguarding Lead's absence.

The Safeguarding and child protection team are:

- Emma Allen, Designated Safeguarding Lead
- Gulsharan McDermott, Safeguarding Deputy
- Terry Hudson, Safeguarding Deputy
- Sue Hillier, Safeguarding Deputy
- Kim Day, Safeguarding Deputy
- Debbie Dow, Safeguarding Deputy

We also have other level three Child Protection trained staff:

- Crystal French (Family Support Practitioner)
- Sarah Potter (Family Support Practitioner)
- Susan Cumbers (Enterprise and Technology Lead)

What to do if:

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

1. Play the situation down; don't make it into a drama.
2. Report to the Headteacher, Deputy Headteachers and/or Enterprise and Technology Lead who will decide on actions including informing parents of any students who viewed the site.
3. Inform the school IT Technician and ensure that site is filtered (LGfL schools report to: **Adept/Atomwide via the LGFL Helpdesk**).

An inappropriate website is accessed intentionally by a student.

1. Report to the Headteacher, Deputy Headteacher and/or Enterprise and Technology Lead who will decide on sanctions/actions including informing parents of any students who viewed the site.
2. Inform the school IT Technician and ensure that site is filtered (LGfL schools report to: **Adept/Atomwide via the LGFL Helpdesk**).

An inappropriate website is accessed intentionally by a staff member.

1. Ensure you have a colleague with you. Do not view the misuse alone.
2. Report to the Headteacher, Deputy Headteacher and/or Enterprise and Technology Lead who will ensure that there is no further access to the device. Record all actions taken.
3. Identify the precise details of the material.
4. Ensure all evidence is stored and logged.
5. Refer to the acceptable use policy agreement that was signed by the staff member, and apply appropriate disciplinary procedure (undertaken by Headteacher).

6. Inform governors of the incident.
7. Inform the school IT Technician and ensure that site is filtered (LGfL schools report to: **Adept/Atomwide via the LGFL Helpdesk**).
- a. In an extreme case where the material is of an illegal nature the Headteacher will contact the local police and follow their advice.

An adult uses school IT equipment inappropriately.

1. Ensure you have a colleague with you. Do not view the misuse alone.
2. Report to the Headteacher, Deputy Headteacher and/or Enterprise and Technology Lead and ensure that there is no further access to the device. Record all actions taken.
3. Ensure all evidence is stored and logged
4. If the material is offensive but not illegal, the Headteacher should then:
 - Remove the device to a secure place.
 - Instigate an audit of all technology equipment by the schools managed service providers or technical teams to ensure there is no risk of students accessing inappropriate materials in the school.
 - Identify the precise details of the material.
 - Take appropriate disciplinary action (undertaken by Headteacher).
 - Inform governors of the incident.
5. In an extreme case where the material is of an illegal nature:
 - The Headteacher will contact the local police and follow their advice.
 - If requested, remove the device to a secure place and document what you have done.

All of the above incidences must be reported immediately to the Headteacher, Deputy Headteacher and/or Enterprise and Technology Lead.

A cyber bullying or a sexting (sharing nudes or semi nudes) incident directed at a student occurs through email or mobile phone technology, either inside or outside of school time.

1. Advise the student not to respond to messages.
2. Report to the Headteacher, Deputy Headteacher and/or Enterprise and Technology Lead who will decide on actions including informing parents of all students involved.
3. Refer to relevant policies including Online Safety, Anti-Bullying and PHSE and apply appropriate sanctions or advice. Also refer to <https://www.gov.uk/government/publications/sharing-nudes-and-semi-nudes-advice-for-education-settings-working-with-children-and-young-people/sharing-nudes-and-semi-nudes-advice-for-education-settings-working-with-children-and-young-people>
4. Follow the direction of the Headteacher or Deputy Headteacher. Staff other than the Headteacher must not attempt to view, share or delete the image or ask anyone else to do so. Actions will be dependent on context and nature of incident and explicit content.
5. Inform the sender's online mail service provider if known.
6. Consider delivering a parent workshop for the school community.
7. Inform the police if necessary.
8. Inform other agencies if required (LA, child protection, adult safeguarding).

Malicious or threatening comments are posted on an Internet site (such as social networking) about a member of the school community (including parents, students and staff).

1. Report to the Headteacher, Deputy Headteacher and/or Enterprise and Technology Lead who will decide on appropriate actions.
2. Inform and request the comments be removed if the site is administered externally.
3. Secure and preserve any evidence.
4. Inform LA and other agencies (child protection, adult safeguarding, governing body etc).
5. Refer to the home/school agreement that was signed by the parent and hold meeting to discuss the issue (if posted by a parent).
6. Send all the evidence to CEOP at <https://www.ceop.police.uk/safety-centre/>

7. Endeavour to trace the origin and inform police as appropriate.
8. Consider delivering a parent workshop for the school community.

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

1. Report to and discuss with the Headteacher, Deputy Headteacher and/or Enterprise and Technology Lead who will decide on actions including informing parents of all students/students involved.
2. Advise the student on how to terminate the communication and save all evidence.
3. Inform LA and other agencies (child protection, adult safeguarding, governing body etc).
4. Contact CEOP <https://www.ceop.police.uk/safety-centre/>
5. Consider the involvement of police and social services.
6. Consider delivering a parent workshop for the school community.

You are concerned that a student's safety is at risk because you suspect they are playing computer games that are inappropriate or certificated beyond the age of the student.

1. Report to and discuss with the Headteacher, Deputy Headteacher and/or Enterprise and Technology Lead who will decide on actions including informing parents of all students/students involved.
2. Advise the student and parents on appropriate games and content. You may want to use LGFL template letters to inform all or targeted parents.
3. If the game is played within school environment, ensure that the IT Technician blocks access to the game.
4. Consider the involvement of social services and/or adult and child protection agencies.
5. Consider delivering a parent workshop for the school community.

You are aware of social network posts and pages created by parents about the school. While no inaccurate information is posted, it is inflammatory and disruptive and staff are finding it hard not to respond.

1. Report to and discuss with the Headteacher, Deputy Headteacher and/or Enterprise and Technology Lead who will decide on actions.
2. Refer to the home/school agreement that was signed by the parent and hold meeting to discuss the issue (if posted by a parent).
3. Contact the poster or page creator and discuss the issues in person.
4. Provide central staff training and discuss as staff how to behave when finding such posts and decide on the appropriate responses.
5. Contact governing body.
6. Consider delivering a parent workshop for the school community.

All of the above incidences must be reported immediately to the Headteacher, Deputy Headteacher and/or Enterprise and Technology Lead.

Students 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.