	Name of School	**South Grove Primary School**
	Guidance review Date	**January 2018**
	Date of next Review	**January 2019**
	Who reviewed this guidance?	**Charlotte Marable Julie Maltwood Brigid Montgomery Sam Puddifoot Charlotte Slade**

Guidance: What do we do if?

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

1. Play the situation down; don't make it into a drama.
2. Report to the Head Teacher/ Designated Safeguarding Lead/ ICT Leader and decide whether to inform parents of any children who viewed the site.
3. Inform the school's ICT technician and ensure the site is filtered (LGfL schools report to: **Atomwide via the LGFL Helpdesk**).
4. Inform the LA if the filtering service is provided via an LA/RBC.

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

1. Refer to the acceptable use policy that was signed by the child, and apply agreed sanctions.
2. Notify the parents of the child.
3. Inform the school's ICT technician and ensure the site is filtered if need be.
4. Inform the LA if the filtering service is provided via an LA/RBC.

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

1. Ensure all evidence is stored and logged
2. Refer to the acceptable use and staffing policy that was signed by the staff member, and apply disciplinary procedure.
3. Notify governing body.
4. Inform the school's ICT technician and ensure the site is filtered if need be.
5. Inform the LA if the filtering service is provided via an LA/RBC.
6. In an extreme case where the material is of an illegal nature:
    a. 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 the misuse immediately to the head teacher/ ICT leader and ensure that there is no further access to the device. Record all actions taken.
3. If the material is offensive but not illegal, the head teacher should then:
    - Remove the device to a secure place.
    - Instigate an audit of all ICT equipment by the school's ICT managed service providers or technician to ensure there is no risk of pupils 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.
4. In an extreme case where the material is of an illegal nature:
    - Contact the local police and follow their advice.
    - If requested to remove the device to a secure place and document what you have done.

All of the above incidences must be reported immediately to the head teacher and ICT leader.

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 policies including e-safety, anti-bullying and PHSE and apply appropriate sanctions.
3. Secure and preserve any evidence through screenshots and printouts.
4. Inform the sender's e-mail service provider if known.
5. Notify parents of all the children involved.
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, LGFL)

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

1. Inform and request the comments be removed if the site is administered externally.
2. Secure and preserve any evidence.
3. Send all the evidence to CEOP at ww.ceop.gov.uk/contact_us.html.
4. Endeavour to trace the origin and inform police as appropriate.
5. Inform LA and other agencies (child protection, Governing body etc).

To consider delivering a parent workshop for the school community

You are concerned that a child'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 child

1. Report to and discuss with BM (the 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 police and social services.
5. Inform LA and other agencies.
6. Consider delivering a parent workshop for the school community.

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

1. Report to and discuss with BM (the child protection officer in school) and contact parents.
2. Advise the child and parents on appropriate games and content.
3. If the game is played within school environment, ensure that the technical team block access to the game
4. Consider the involvement social services 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. Contact the poster or page creator and discuss the issues in person
2. Provide central staff training and discuss as a staff how to behave when finding such posts and appropriate responses.
3. Contact governing body and parent association
4. Consider delivering a parent workshop for the school community.

All of the above incidences must be reported immediately to the head teacher and ICT leader.

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.

Guidance: What do we do if?

User Signature

I agree to abide by all the points above.

I understand that I have a responsibility for my own and others e-safeguarding and I undertake to be a 'safe and responsible digital technologies user'.

I understand that it is my responsibility to ensure that I remain up-to-date and read and understand the school's most recent e-safety policies.

I understand that failure to comply with this agreement could lead to disciplinary action.

Signature ..... Date .....

Full Name ..... (printed)