



Houghton Conquest Lower School and Pre-school

Online Safety Policy

The requirement to ensure that children and young people are able to use the internet and related communications technologies appropriately and safely is addressed as part of the wider duty of care to which all who work in schools are bound. Schools must, through their online safety policy, ensure that they meet their statutory obligations to ensure that children and young people are safe and are protected from potential harm, both within and outside school. The policy will also form part of the school's protection from legal challenge, relating to the use of digital technologies.

Due to the ever changing nature of digital technologies this online safety policy will be reviewed at least annually and, if necessary, more frequently in response to any significant new developments in the use of the technologies, new threats to online safety or incidents that have taken place.

Scope of the Policy

At Houghton Conquest Lower School, we recognise the value that Information Systems have on education and learning and seek to ensure that this can be done in a safe environment, which fosters enthusiasm for knowledge.

This policy applies to all members of the school (including staff, children, volunteers, governors, parents / carers, visitors and community users) who have access to and are users of school ICT systems, both in and out of the school.

The Education and Inspections Act 2006 empowers Headteachers to such an extent as is reasonable, to regulate the behaviour of children when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, or other online safety incidents covered by this policy, which may take place outside of the school, but is linked to membership of the school. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data.

The school will deal with such incidents within this policy, associated behaviour and anti-bullying policies and will, where known, inform parents / carers of incidents of inappropriate online safety behaviour that take place in and out of school.

Roles and Responsibilities

The Governing Body

Governors are responsible for the approval of the online safety policy and for reviewing the effectiveness of the policy. This will be carried out by the Governors receiving regular information about online safety incidents and monitoring reports.

Headteacher

The Headteacher is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.

- The Headteacher and another member of the Senior Leadership Team should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff. (Annex A: flow chart “Responding to incidents of misuse”).
- The Headteacher has a duty of care for ensuring the safety (including online safety) of members of the school community, though the day to day responsibility for online safety will be delegated to the Online Safety Coordinator.

The Designated Safeguarding Lead

Details of the school’s Designated Safeguarding Lead (DSL) and deputy are set out in our Safeguarding and Child Protection policy.

The DSL takes lead responsibility for online safety in school, in particular:

- Working with the Online Safety Coordinator and other staff, as necessary, to address any online safety issues or incidents.
- Ensuring that any online safety incidents are logged (see Annex B) and dealt with appropriately in line with this policy.
- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school Behaviour Policy.

Online Safety Coordinator / Officer (School Business Manager):

- Leads online safety in school.
- Takes day to day responsibility for online safety issues and has a leading role in establishing and reviewing the school online safety policies / documents.
- Ensures that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place.
- Provides training and advice for staff.
- Liaises with the Local Authority / relevant body.
- Liaises with IT support team.
- Receives reports of online safety incidents and creates a log of incidents to inform future online safety developments.
- Attends relevant meeting / committee of governors.
- Reports regularly to Senior Leadership Team.

All staff and Volunteers

All staff, including agency staff, and volunteers are responsible for:

- Having an up to date awareness of online safety matters and of the current school Online Safety Policy and practices.
- Working with the appropriate member of staff to ensure that any online safety incidents are logged (Annex B) and dealt with appropriately in line with this policy.
- Ensuring that online safety issues are embedded in all aspects of the curriculum and other activities.
- Monitoring the use of digital technologies, mobile devices, cameras etc in lessons and other school activities (where allowed) and implement current policies with regard to these devices.
- In lessons where internet use is pre-planned children should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches. *Additionally children should be regularly reminded about using “safe search” in Google and how to check if it is turned on.*

- In lessons where the internet is used, the class teacher needs to educate the children on the process that they need to follow when dealing with any unsuitable material:
 - The child tell an appropriate adult that there is something inappropriate on their computer and closes the lid or turns the screen off. Children should be reminded not to turn the computer off.
 - The adult checks the relevant computer and if reports it using annex B to the Online Safety Coordinator.
- Providing online safety in lessons and utilise appropriate references. Staff will participate in Safer Internet Day (SID) (February).

Education - Parents / Carers

Some parents and carers may have only a limited understanding of online safety risks and issues, yet they play an essential role in the education of their children and in the monitoring / regulation of the children's online behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

The school will raise parents' awareness of online safety in letters, other communications home, parents' evenings and information via our website.

- If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the class teacher and then depending on the concern the Headteacher or the deputy DSL. Staff to complete Annex C as necessary to record any incidents reported to school by parents.
- Concerns or queries about this policy can be raised with any member of staff or the Headteacher.

Parents and carers will be encouraged to support the school in promoting good online safety practice and to follow guidelines on the appropriate use of:

- Digital and video images taken at school events.

Parents can seek further guidance on keeping children safe online from the following organisations and websites:

- What are the issues?, UK Safer Internet Centre: <https://www.saferinternet.org.uk/advice-centre/parents-and-carers/what-are-issues>
- Hot topics, Childnet International: <http://www.childnet.com/parents-and-carers/hot-topics>

Education – children / pupils

Whilst regulation and technical solutions are very important, their use must be balanced by educating children to take a responsible approach. The education of children in online safety is therefore an essential part of the school's online safety provision. Children and young people need the help and support of the school to recognise and avoid online safety risks and build their resilience.

Online safety should be a focus in all areas of the curriculum and staff should reinforce online safety messages across the curriculum. The online safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:

- A planned online safety curriculum should be provided as part of Computing / PHSE / other lessons and should be regularly revisited.
- Children's progress will be recorded using the school's electronic assessment tools.
- Key online safety messages should be reinforced as part of a planned programme of assemblies and pastoral activities.
- Children should be taught in all lessons to be critically aware of the materials / content they access online and be guided to validate the accuracy of information.
- Children should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.
- Staff should act as good role models in their use of digital technologies the internet and mobile devices.

- The school will use assemblies to raise pupils' awareness of the dangers that can be encountered online and may also invite speakers to talk to pupils about this.

The school will use a variety of websites in order to approach the many different aspects of the curriculum. Some of these websites are listed below:

- <https://scratch.mit.edu/>
- <https://www.thinkuknow.co.uk/>
- <http://www.bbc.co.uk/bitesize/ks2/>

Education & Training – Staff / Volunteers

It is essential that all staff receive online safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- All staff will receive relevant online safety training.
- The Online Safety Coordinator will receive regular updates through attendance at external training events and by reviewing guidance documents released by relevant organisations.
- External resources on internet safety are available at <https://www.saferinternet.org.uk/safer-internet-day/safer-internet-day-2019/education-packs>.
- It is accepted that from time to time, for good educational reasons, children may need to research topics (eg racism, drugs, and discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the ICT support team (or other relevant designated person) temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need.

Education/Training – Governors

Governors should take part in online training / awareness sessions. This may be offered in a number of ways:

- Attendance at training provided by the Local Authority / National Governors Association / or other relevant organisation.
- Participation in school training / information / assemblies for staff or parents.

Cyber-bullying

Definition

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of one person or group by another person or group, where the relationship may involve an imbalance of power.

Preventing and Addressing Cyber-Bullying

To help prevent cyber-bullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

The school will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes personal, social, health and economic (PSHE) education, and other subjects where appropriate.

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school anti bullying policy.

The DSL will consider whether the incident should be reported to the police if it involves illegal material, and will work with external services if it is deemed necessary to do so.

Use of digital and video images

- In accordance with guidance from the Information Commissioner's Office, parents / carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use is not covered by the Data Protection Act). To respect everyone's privacy and in some cases for protection reasons, these images should not be published / made publicly available on social networking sites, nor should parents / carers comment on any activities involving other children in the digital / video images. Parents must sign a photograph consent form to take photographs of their child/children at school events after reading our 'Use your camera and video courteously code'.

Inappropriate content and language

The policy provides the following definitions of what is deemed 'inappropriate' for both email and website use.

Inappropriate email content:

abusive	bullying	defamatory
disruptive	harmful to council, LA or school morale	harassing
insulting	intolerant	obscene
offensive*	politically biased**	sexual innuendo
violent	threatening	

*e.g. material that can be construed as offensive on the grounds of gender, race, ethnicity, disability, sexuality, religion, age, size/stature, status, TU membership.

**no partiality towards or against any political grouping or individual

The type of language that is used in emails should be no different to that which is used in face to face situations.

Inappropriate web content:

Adult or explicit material	Incitement (e.g. racism)
Chat rooms/instant messaging (except that promoted by the school for educational purposes)	Personal ads Dating
Criminal skills/resources	Newsgroups/forums (except that promoted by the school for educational purposes)
Downloads of ring tones, screensavers and games (except any promoted by the school for educational purposes)	Internet peer to peer networks
Downloads of freeware, shareware, evaluation packages (except by authorised persons and in compliance with copyright law)	Hacking, virus writing, password cracking
Illegal drugs	Tasteless and offensive content
Gambling	Depiction/advocation of violence or use of weapons

Monitoring Arrangements

The DSL monitors behaviour and safeguarding issues related to online safety. An incident report log can be found in Annex B. An incident report log for issues reported by parents can be found in Annex C

Schedule for Development / Monitoring / Review

This online safety Policy (OSP) was approved by the <i>Governing Body</i>	<i>January 2019</i>
The implementation of this OSP will be monitored by the:	Online Safety Coordinator (School Business Manager)
Monitoring will take place at regular intervals:	<i>Annually or as required</i>
Should serious online safety incidents take place, the following external persons / agencies should be informed:	<i>LA ICT Manager, LA Safeguarding Officer, Police</i>

The school will monitor the impact of the policy using:

- Logs of reported incidents
- Monitoring logs of internet activity (including sites visited)
- Internal monitoring data for network activity

References

www.thinkuknow.co.uk

<https://www.saferinternet.org.uk/safer-internet-day/safer-internet-day-2019/education-packs>

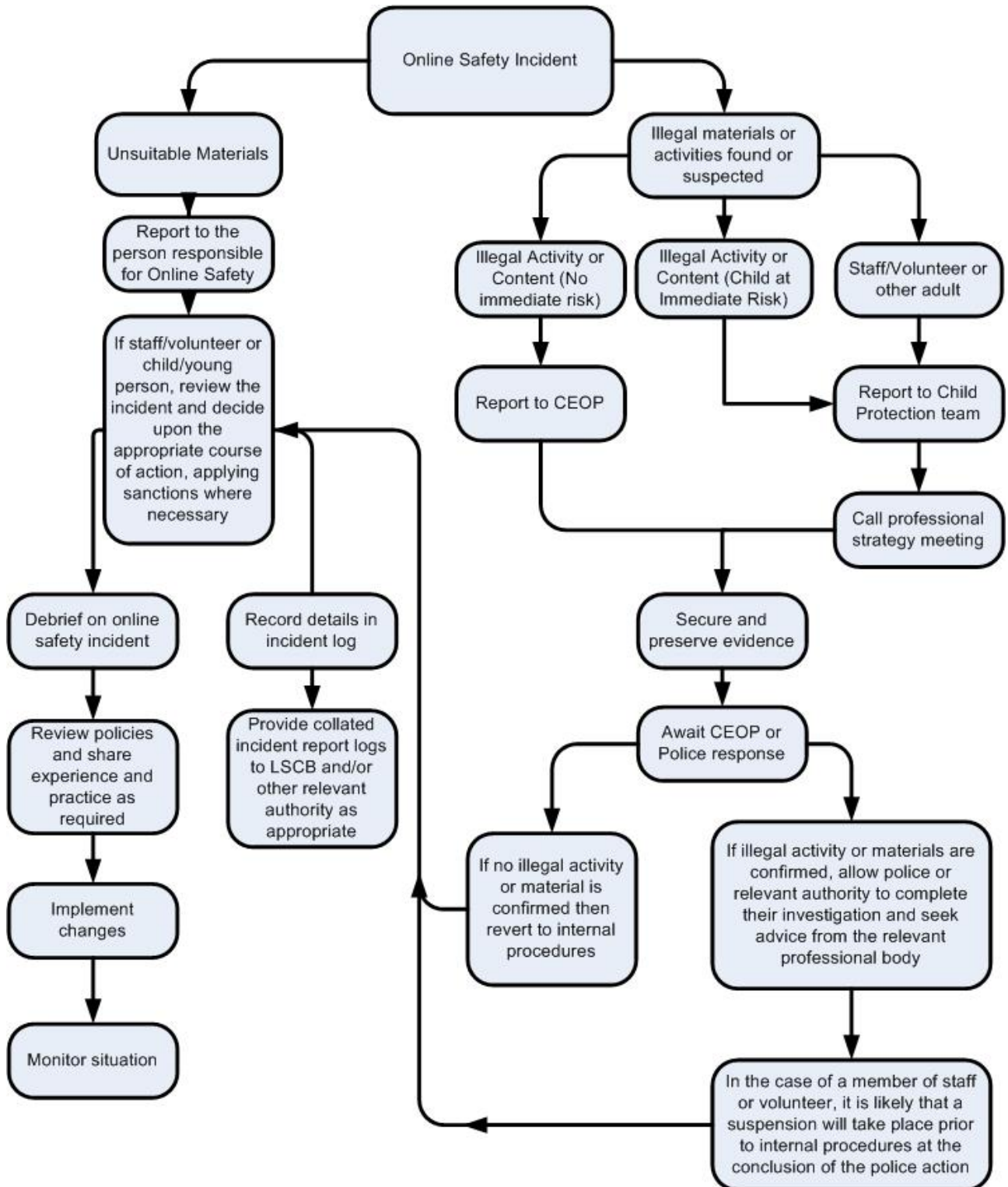
<https://www.saferinternet.org.uk/advice-centre/parents-and-carers/what-are-issues>

<http://www.childnet.com/parents-and-carers/hot-topics>

This online safety policy is linked to our
Anti-Bullying Policy
Anti-Racist policy
Behaviour Policy
British Values Policy
Safeguarding and Child Protection Policy
Prevent Policy
PSHCE Policy
Social Media Policy
Acceptable User policy

Annexes

Annex A: Responding to incidents of misuse



Annex B: Online Safety Incident Report Log

Online Safety incident report log				
Date	Where the incident took place	Description of the incident	Action taken	Name and signature of staff member recording the incident

Annex C: Online Safety Incident Report Log (Parents)

Online Safety incident report log				
Date	Where the incident took place / name of parent reporting	Description of the incident	Action taken	Name and signature of staff member recording the incident