Hill House International Junior School

Online Safety POLICY

Online Safety Policy

1 Scope

1.1 This policy is addressed to all members of the School community. A copy of the policy is available to parents on request and the School actively promotes the participation of parents to help the School safeguard the welfare of pupils and promote the safe use of Information and Communications Technologies (ICT).
The policy has been agreed by senior management and approved by Proprietors.

The school's Designated Safeguarding Lead is Mr Chris Carlson.
The school's Online Safety Coordinator is Mr Andrew Hepburn.
The Online Safety Policy and its implementation will be reviewed annually.

1.2 This policy relates to all communications devices, network hardware and software and services and applications associated with them in use at the School including:

1.2.1 the internet

1.2.2 e-mail

1.2.3 mobile phones and smartphones

1.2.4 desktops, laptops, netbooks, tablets/phablets

1.2.5 personal music players

1.2.6 devices with the capability for recording and / or storing still or moving images

1.2.7 social networking, micro blogging and other interactive web sites

1.2.8 instant messaging (including image and video messaging via apps such as SnapChat and WhatsApp), chat rooms, blogs and message boards

1.2.9 webcams, video hosting sites (such as YouTube)

1.2.10 gaming sites

1.2.11 SMART boards

1.2.12 other photographic or electronic equipment.

1.3 It applies to the use of any of the above on School premises and also any use, whether on or off School premises, which affects the welfare of other pupils or any member of the School community or where the culture or reputation of the School are put at risk.

1.4 The School is committed to safeguarding the welfare of all pupils and an effective ICT safety strategy is paramount to this. The aims of this policy are to:

1.4.1 encourage pupils to make good use of the educational opportunities presented by access to ICT;

1.4.2 safeguard and promote the welfare of pupils, in particular by anticipating and preventing the risks arising from:

(a) exposure to inappropriate material (such as pornographic, racist, extremist or offensive materials);

(b) the sharing of personal data, including images;

(c) inappropriate online contact; and

(d) cyberbullying and other forms of abuse;

1.4.3 minimise the risk of harm to the assets and reputation of the School;

1.4.4 limit the risks that children and young people are exposed to when using ICT;

1.4.5 ensure that pupils use ICT safely and securely and are aware of both external and peer to peer risks when using ICT.

2 Roles and responsibilities

2.1 Proprietors

2.1.1 The Proprietors of the School have overall responsibility for the safeguarding procedures within the School.

2.1.2 The Proprietors will undertake an annual review of the School's safeguarding procedures and their implementation, which will include consideration of how pupils may be taught about safeguarding, including online safety, through the School's curricular provision, ensuring relevance, breadth and progression.

2.1.3 The Designated Safeguarding Lead is responsible for the online safety of pupils.

2.1.4 The Designated Safeguarding Lead is responsible for managing online safety incidents in the same way as other safeguarding matters in accordance with the School's Safeguarding and Child Protection Policy and Procedures, including the keeping and monitoring of the Online Safety Incident Log.

2.1.5 The Designated Safeguarding Lead will work with the Online Safety Coordinator in monitoring the School's Online Safety practices and the implementation of the procedures to assess whether any improvements can be made to ensure the online safety and wellbeing of pupils.

2.1.6 The Proprietors and other senior management will be updated regularly by the Designated Safeguarding Lead on the operation of the School's safeguarding arrangements, including online safety practices.

2.2 Online Safety Coordinator

2.2.1 The Online Safety Coordinator is responsible for the operation of the School's filtering system to ensure that pupils are unable to access any material that poses a safeguarding risk, including terrorist and extremist material, while using the School's network.

2.2.2 The Online Safety Coordinator is responsible for ensuring:

(a) that the School's technical infrastructure is secure and is not open to misuse or malicious attack;

(b) that users may only access the School's networks and devices if properly authenticated and authorised;

(c) that the filtering policy is applied and updated on a regular basis;

(d) that the use of the School's networks and devices is regularly monitored to ensure compliance with this Policy and that any misuse or attempted misuse can be identified and reported to the appropriate person for investigation; and

(e) that monitoring software and systems are kept up to date.

2.2.3 The Online Safety coordinator will:

(a) keep up to date with the latest risks to children whilst using technology;

(b) Liaise regularly with the Designated Safeguarding Lead;

(c) Ensure anti-virus software is up to date, fit for purpose and is applied to all appropriate devices.

(d) Ensure passwords are applied correctly to all users, regardless of age.

2.3 **All staff**

2.3.1 The School's staff have a responsibility to act as good role models in their use of technologies, the internet and mobile electronic devices.

2.3.2 Staff are expected to follow the School's staff Acceptable Use Policy which is available in the Staff Handbook.

2.3.3 Staff have a responsibility to report any concerns about a pupil's welfare and safety in accordance with this policy and the School's Safeguarding and Child Protection Policy and Procedures.

3 Education and training

3.1 Online Safety is integral to the School's ICT curriculum. The safe use of ICT is also a focus in all areas of the curriculum and key Online Safety messages are reinforced as part of tutorial / pastoral activities, teaching pupils at an age-appropriate level:

3.1.1 about the risks associated with using the internet and how to protect themselves and their peers from potential risks;

3.1.2 to be critically aware of content they access online and guided to validate accuracy of information;

3.1.3 how to recognise suspicious, bullying or extremist behaviour;

3.1.4 the definition of cyberbullying, its effects on the victim and how to treat each other's online identities with respect;

3.1.5 the consequences of negative online behaviour; and

3.1.6 how to report cyberbullying and / or incidents that make pupils feel uncomfortable or under threat and how the School will deal with those who behave badly.

3.2 The School provides Online Safety training to staff to protect pupils and themselves from online risks and to deal appropriately with Online Safety incidents if or when they occur. Ongoing staff development training includes training on online safety together with specific safeguarding issues including cyberbullying and radicalisation. The frequency, level and focus of such training will depend on individual roles and requirements.

4 School rules and procedures

4.1 The expectations for pupils using the computers and the Internet are set out in the School's Pupil Acceptable Use Policy, which is signed, by parents and pupils.

4.2 Any misuse of ICT by pupils will be dealt with under the School's Behaviour Policy.

4.3 Bullying incidents involving the use of ICT will be dealt with under the School's Anti-bullying Policy.

4.4 If there is a suggestion that a child is at risk of abuse or significant harm, the matter will be dealt with under the School's child protection procedures (see the School's Safeguarding and Child Protection Policy and Procedures).

4.5 In a case where the pupil is considered to be vulnerable to radicalisation they will be referred to the Channel programme. Channel is a programme which focuses on support at an early stage to people who are identified as being vulnerable to being drawn into terrorism.

5 Parents

5.1 The role of parents in ensuring that pupils understand how to stay safe online is crucial. The School expects parents to promote safe online practice and to:

5.1.1 support the School in the implementation of this policy and report any concerns in line with the School's policies and procedures;

5.1.2 talk to their child to understand the ways in which they are using the internet, social media and their mobile devices and promote responsible behaviour; and

5.1.3 encourage their child to speak to someone if they are being bullied or need support.

5.2 Parent's attention will be drawn to the school Online Safety Policy in newsletters and on the school website.

5.3 If parents have any concerns or require any information about Online Safety, they should contact the Designated Safeguarding Lead.

5.4 **Useful resources for parents**

http://www.saferinternet.org.uk/

http://www.kidsmart.org.uk

http://www.safetynetkids.org.uk/

http://www.safekids.com/

http://www.thinkuknow.co.uk

DfE's Advice for Parents and Carers on Cyberbullying

http://parentinfo.org/

DfE's Advice on the use of social media for online radicalisation

The Local Safeguarding Children Board has produced guidance for parents on radicalisation, which is available here:
https://www.rbkc.gov.uk/subsites/lscb/parentscarersandthepublic/radicalisation.aspx

6 Monitoring and review

6.1 All Online Safety incidents will be logged in the Online Safety Incident Log.

6.2 The Designated Safeguarding Lead has responsibility for the implementation and review of this policy and will consider the record of Online Safety incidents and the logs of internet activity (including sites visited) as part of the ongoing monitoring of safeguarding procedures, to consider whether existing security and Online Safety practices within the School are adequate.

6.3 Consideration of the efficiency of the School's Online Safety procedures and the education of pupils about keeping safe online will be included in the Proprietors' annual review of safeguarding.

7 Technical and Hardware Guidance

The School uses a range of devices including desktop computers and laptops.
In order to safeguard the student and in order to prevent loss of personal data we employ the following assistive technology:

7.1 Internet Provision

7.1.1 The School's Internet Service Provider is Focus Media.

7.2 Content Filtering and Monitoring

7.2.1 The School uses Smoothwall filtering and monitoring that prevents unauthorised access to illegal websites. It also prevents access to inappropriate websites; appropriate and inappropriate is determined by the age of the user and will be reviewed in line with this policy or in response to an incident, whichever is sooner.

7.3 Downloading Files and Applications

7.3.1 Pupils are not permitted to download any material from the Internet unless directed to do so by an appropriate staff member.

8 Safe Use

8.1 Internet

8.1.1 Internet use will be granted: to staff upon signing the Staff Acceptable Use Policy; students upon signing and returning their acceptance of the Pupil Acceptable Use Policy.

8.1.2 The School maintains that pupils will have supervised access to Internet resources through the school's fixed and mobile Internet technology. All staff will preview any recommended sites before use.

8.1.3 Raw image searches are discouraged when working with pupils. If Internet research is set for homework, specific sites will be suggested that have previously been checked by the teacher. It is advised that parents recheck these sites and supervise this work. Parents will be advised to supervise any further research.

8.1.4 All users must observe software copyright at all times. It is illegal to copy or distribute school software or illegal software from other sources. All users must observe copyright of materials from electronic resources.

8.2 E-Mail

8.2.1 All staff are reminded that emails are subject to Freedom of Information requests, and as such the email service is to be used for professional work-based emails only. Emails of a personal nature are not permitted. Similarly use of personal email addresses for work purposes is not permitted.

8.2.2 Pupils are not permitted to access personal e-mail accounts whilst at school.

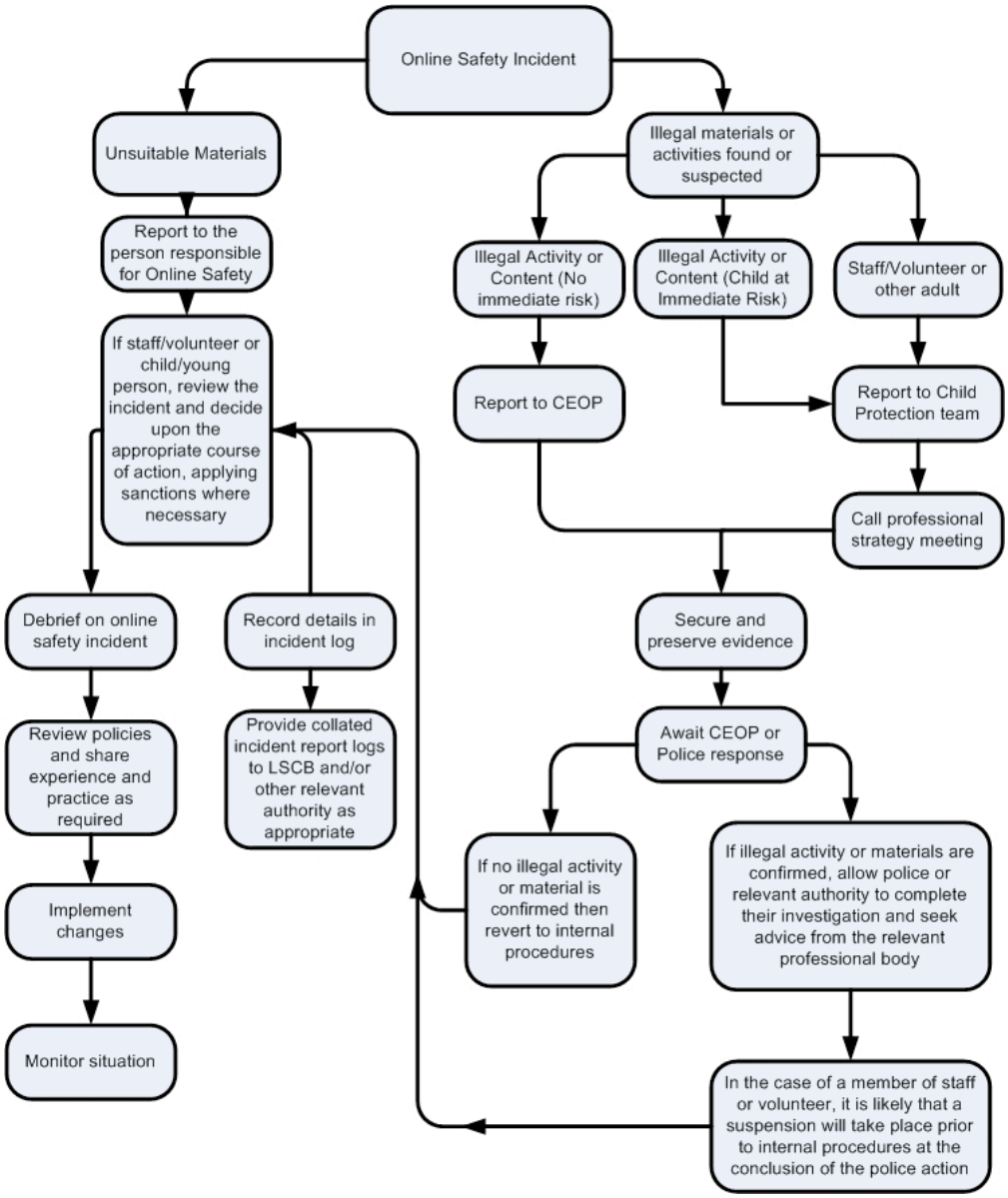
8.3 Social Media

8.3.1 Use of social networking sites and newsgroups in the school, is not allowed and will be blocked/filtered.

8.3.2 Pupils will be advised never to give out personal details of any kind that may identify themselves, other pupils, their school or location.

8.3.3 Parents, pupils and staff will be advised of the dangers of discussing pupils, staff or the school on social networking sites.

Online Safety Incident Flowchart



Authorised by	**Resolution of the Proprietors**
Signed on behalf of the Proprietors	**William Townend**
	……
Date	**21 September 2018**

Effective date of the policy	**21 September 2018**
Review date of the policy	**21 September 2019**