REVIEWED: OCTOBER 2017
NEXT REVIEW DATE: AUTUMN 2018
REVIEWED BY: ASSISTANT HEAD (DSL)
RATIFIED BY: COMPLIANCE COMMITTEE

Hazelwood School

E-SAFETY POLICY

This Policy includes the Nursery and Early Years Foundation Stage

The very nature of this subject means that this Policy must be as dynamic as possible and in constant review. The devices themselves, new networks and the terminology associated with technology are developing all the time.

This Policy should be read alongside the Relationships and Sex Education Policy.

The School has an eSafety Committee and a designated eSafety Officer who is also the Named Lead DSL

Hazelwood is sufficiently flexible to manage new and emerging technologies, and encourages children to use new technology, which includes electronic tools or other such electronic devices, as they have important educational and social benefits. Our Policy aims to balance the desirability of fully exploiting the vast educational potential of new technologies with providing safeguards against risks and unacceptable material and activities.

This Policy considers all technological appliances that have been provided by the School. Although a child may be trusted by their parents with regard to private internet use, the School has a duty to safeguard them and other children. Parents need to be reassured that their child is not able to access material deemed unsuitable and/or in contravention of the School's Acceptable Use Policy (AUP) whilst in School.

Aims/Targets/Rationale/Issues

Children are keen to grasp the opportunities offered by new technology. However, any new technology has associated risks which include the following: exposure to inappropriate material, physical danger, online/cyber bullying, legal and commercial issues, personal financial gain and gambling. The aims of this Policy are:

- To promote the welfare and safeguarding of pupils and staff at Hazelwood, including against radicalisation.
- To ensure that pupils are ICT literate and can use the facilities to ensure that their educational provision is enhanced to the maximum.
- To promote responsible and effective use of electronic communication (including the use of the internet and mobile phone technology).
- To educate pupils and staff about the risks and responsibilities involved in the use of new technology, particularly with regard to the potential moral and criminal consequences of their actions.
- To raise awareness of and counter instances of cyber-bullying. This includes bullying via text message, via instant-messenger services and social network sites, via email, and via images or videos posted on the internet or spread via mobile phone. It can take the form of type of bullying, i.e. technology can be used to bully for reasons of

race, religion, sexuality, disability, etc.

- That safeguarding is taught online, through the curriculum and PSHE and personal, social, emotional development in the Early Years Foundation Stage. The School should help children to adjust their behaviours in order to reduce risks and build resilience, including to radicalisation, particularly when using electronic equipment and internet.

The existence of the many and various forms of electronic equipment, in any environment, raises issues of security and personal responsibility, not only in terms of its appropriate use but also for its safe keeping.

Personal electronic equipment may be used onsite provided it complies with the eSafety Policy and AUP, all such equipment must be approved by a member of the ICT staff before connecting it to the School network. Consideration of Virus Checkers will be taken into account. No images of children may be stored on these devices or pupils personal data and the School takes no responsibility for loss or damage, however caused.

Procedures and Practices, Rules and Regulations, Measures in place to support the Policy:

Years 1-8

The School provides every child with access to the internet and the School's own network. Each child in Year 1 and above has their own individual username and password with the means to create and save files. Keeping Children Safe in Education (2016) has been important in formulating this Policy.

Wifi is deployed across the School, which has the same level of filtering as the wired network. Our filtering system restricts access to inappropriate materials for any device attached to the School network, we have safer use protocols and monitoring procedures including desktop monitors in operation on all pc's.

All staff mobile phones and personal technology devices on which images of children may be taken are registered at School with the Bursar's PA as per the 'Taking Storing and Using Images of Children Policy'. This register will be regularly updated as devices are replaced.

The rules and regulations below are not meant to act as an exhaustive list of "dos and don'ts"; rather to offer a level of consistency and guidance across each area of the School. These are to be read in conjunction with the main AUP and, where appropriate, the iPad AUP.

- Pupils may only use the account assigned to them and must not share their password with anyone.
- Pupils are not allowed to email each other or a member of staff unless it is school related. Emailing outside bodies is allowed with permission of the member of staff (examples may include pen pals), the School reserves the right to restrict individual users or groups to internal emailing only and this is available through the Google Apps platform.

- Air Dropping and iPad communication is closely monitored with iPad Form Time Inspections and rules/reminders about appropriate use provided.
- Chat rooms and social networking sites/Apps are not permitted.
- Gambling and eCommerce are not permitted.
- Downloading or sharing of files such as music files are not permitted on the computer, although Upper School children with iPads have permission to download a small amount of music.
- The use of inappropriate images/websites/video clips are not permitted.
- Pupils should not post images of themselves or others online.
- Pupils should not share information about themselves online which includes a surname, location or other identifiable markers without prior permission of a teacher. This should only be in a secure location including the School VLE, closed blogs or other approved sites, even then children should use this a learning experience and should be taught to question why the information is needed.
- Pupils should not share their iPads or take another person's iPad for any reason, unless instructed to do so by a teacher.
- Cyber Bullying and any misuse of ICT should be passed immediately to the Deputy Head (Pastoral) or DSL. For further information on Cyber Bullying see the separate policy.
- eSafety Evenings are offered to parents and guardians on advice to be applied at home.
- eSafety is taught to pupils from Year 1 in their ICT lessons. eSafety is also incorporated in our daily approach.

Early Years Foundation Stage

Our filtering system restricts access to inappropriate materials for any device attached to the School network, we have safer use protocols and monitoring procedures including desktop monitors in operation on all pc's.

- Children will only be given access to age-related programs and only access other information on the internet under the supervision of a member of staff.
- All devices connected to the School network have filters in place.
- Staff will only use School devices (cameras, iPads) for taking images of children. Staff personal mobile phones/devices are locked away and are not used in the presence of children unless in an emergency.
- eSafety is introduced to the children in an age-appropriate manner. It is planned into programs of study from Oak Reception.
- eSafety Evenings are offered to parents and guardians on advice to be applied at home.

It is recognised that the internet is a rapidly evolving and largely unregulated arena. Whilst the Department for ICT works proactively to ensure eSafety measures guard against inappropriate content, maintaining pace with inappropriate content and eSafety threats does sometimes force a reactive approach after an event occurs. Should a pupil be exposed to inappropriate content, direct consultation between the Head, Deputy Head (Pastoral), and Head of ICT or DSL/eSafety Officer will occur to ensure an appropriate and timely response based upon the pastoral welfare needs of the individual child.

1. Paperwork - The AUP
This protects all parties by clearly stating what is acceptable and what is not. This is signed by a parent or legal guardian on behalf of their child when they join the School. Pupils passwords may be passed to parents upon request. We ask that they discuss this content with the child before signing and returning it. Staff members are required to read and sign this document before using any ICT at Hazelwood School.

2. Monitoring
Although staff and pupils at Hazelwood have signed the AUP to say they will adhere to certain rules whilst using school technology, the School's ICT system is monitored and managed in a number of ways designed to protect users and identify misuse, specifically:

- Desktop monitoring is in place (pc's only) which takes screenshots when key words are used. This records both bad language and bullying and acts as a deterrent.
- Internet filtering is used to make the internet as safe as possible in the School's opinion. The level of filtering is tiered so the youngest children only have access to a few selected sites, whilst as the pupils get older the sites are less restricted and they are taught to use them sensibly. Staff have a higher level of access.
- Pupils and staff can suggest sites for unblocking and consideration will be taken to consider it if appropriate. Suspicious searches are checked at least once daily for staff and pupils.
- All users from Year 1 upwards have their own private usernames and password. This means that anything done during a user's login session can be attributed to them.
- Pupil's gmail accounts and messaging system are monitored and any suspect words included in their email will involve the email being forwarded to the DSL/eSafety Officer.
- The School can and does remotely monitor the use of apps on the iPads and monitor app installation even when the iPad is not on site.

Monitoring is carried out by the eSafety Officer and ICT manager, both of whom report to the Deputy Head (Pastoral) and DSL immediately that any suspicious or notable material is noted. Both have access to the filtering to provide a cross-check against abuse of the system by staff.

3. Whole Staff
It is the responsibility of the whole staff to report any concerns regarding inappropriate use of ICT to the Head of ICT or the DSL or Assistant Head (with responsibility for Early Years).

No pupil should be using the School's ICT without a member of staff being present, except when 1:1 iPads issued by the School are taken home.

4. eAwareness and eSafety: Teaching and Learning Summary
Cyber-bullying, safe use of the Internet and appropriate use of technologies are addressed in PSHE lessons as well as invited guest speakers and other events.

Pupils are taught about eSafety regularly in lessons including the use of thinkuknow.co.uk

starting with the children in Oak Reception. This is repeated with more discussion in Years 1 and 2 before being built more into their ongoing lessons for the remaining year groups. A key part of this message is the need for the pupils to talk to staff when there is a problem, with the older children reference will also be made to the CEOP reporting tool on HALO.

Working with a specialist internet education outside agency with a background of over 20 years police in vice with specific reference to internet safety, children in Years 4,5,6,7 and 8 receive 45 minute tailor made presentation at the beginning of the Spring term. This alerts them to the possible dangers of the internet using age appropriate scenarios, examples and high impact visual material. These presentations are followed with an evening presentation to parents which reinforces the content and informs them of the possible dangers and their responsibilities regarding their children's internet safety.

Summary notes from the meeting are also available for all parents.

Pupils should be aware that any IT hardware or data can be inspected or viewed by any member of staff whilst on site as permitted under Section 2 subsections 6E and 6F of the Education Act 2011.

When a child leaves the site their ICT use becomes the responsibility of their parents. However, the School would treat it very seriously should a child access or share inappropriate content or post comments on the internet that reflect badly on the School or targets individual students or staff members.

- Most initial offences will be dealt with by the Deputy Head (Pastoral) who will liaise with relevant staff, including eSafety Officer and DSL if appropriate
- More serious offences or repeated abuse of ICT by a pupil will be dealt with by the Head.

5. Extremist material

Extremist material and access to it is an increasing national threat and the School takes its responsibility in protecting the School and pupils seriously.

The School filters, screen captures and email filters help protect the pupils by blocking inappropriate content and flagging worrying behaviour in this area to the DSL. The DSL will report any concerns to the relevant agencies in line with the *Safeguarding and Child Protection Policy*.

Teaching and Room Staff on the Hazelwood Nursery and Early Years (HNEY) site undergo training to raise their awareness of the risks posed by online activity of extremist and terrorist groups and to help support and protect the children in their care. A register of this training is maintained by the School.

eSafety training (mentioned in section 4) includes material on who to approach and how to seek help.

Acceptable Use Guidelines for Pupils

You are expected to show *safe* and *respectful* use of our digital learning facilities in line with our School Values:

Think before you click … guidelines for safer internet, email and computer use.

- I will only use the School computers for my schoolwork, homework and as directed by my teachers.

- I will only use the School computers when a member of staff is present and has given me permission.

- I will only email and message people within the Hazelwood Community. The messages I send will be polite and respectful.

- I will always ask permission before printing.

- I will not use my own memory stick, laptop or mobile device unless I have been given permission by a teacher.

- If I see anything I am unhappy with or I receive a message I do not like, I will not respond directly to it. Instead I will report it to a teacher to protect myself and others.
- I will not provide my home address, phone number, send a photograph or video, or give any other personal information that could be used to identify me, my family or my friends, to anyone online unless my teacher has given me permission.
- I will not download and store images, music or video files unless I have permission to do so.
- I understand that the School network is monitored to provide safe learning for pupils.
- I will not refer to the School in any social media activity.

To be used in conjunction with iPad AUP Policy, School AUP, Cyber-bullying and Relationships and Sex Education Policy.

Ratified by the Compliance Committee 10th November 2017