



Hazelwood Schools

Online Safety Policy

Reviewed and Adopted: **October 2017**

Reviewed by: HT/LTS Committee

Next Review: October 2020

Review every three years

1. Introduction

It is recognised by Hazelwood Schools that the use of technology presents particular challenges and risks to children and adults both inside and outside of school.

Hazelwood Schools identifies that the issues classified within online safety are considerable, but can be broadly categorised into three areas of risk:

- **content:** being exposed to illegal, inappropriate or harmful material
- **contact:** being subjected to harmful online interaction with other users
- **conduct:** personal online behaviour that increases the likelihood of, or causes, harm

The internet is an essential element of life in the 21st Century; it is also a part of the statutory curriculum and a necessary tool for staff and children, therefore we have a duty to provide children with quality internet access as part of their learning experience.

- Internet access is designed specifically for pupil use and includes filtering appropriate to the age of pupils
- Pupils are made aware of what constitutes acceptable internet use and what doesn't
- Pupils are educated in the effective use of the internet in research, including the skills of knowledge location, retrieval and evaluation as well as compliance with copyright law

There are certain aspects of the above that are particularly challenging for vulnerable pupils with additional needs. Pupils, with additional needs may have needs that could present a range of challenges for effective online safety.

We will consider their online safety needs in relation to specific adaptations that may be required for such pupils. The SENDCo, along with class teachers have a role in coordinating the development of a child centred strategy that would apply to specific needs.

2. Background

Since 2015, preventing pupils viewing unsuitable materials has no longer been simply a moral obligation for educationalist. The Counter Terrorism and Security Act 2015 requires educational establishments to provide security measures to prevent the radicalisation of young people by groups that use the internet to publish extremist ideology.

Online safety is concerned with educating pupils about the benefits and risks of:

- Internet technologies, via iPads, laptops, desktop computers, gaming devices etc.
- Electronic communications such as mobile phones and other internet enabled devices and technology
- Social media and personal publishing

It is also about providing safeguards and awareness for children to enable them to be in better control of their online experience.

3. Online Safety Policy

An effective Online Safety Policy is dependent on effective practice at various levels including:

- Responsible ICT use by all staff, children and young people; reinforced by awareness raising and published policies
- All staff, have read annex C regarding Online Safety within 'Keeping children safe in education' 2016.
- External Online Safety experts delivering annual training to all staff
- Providing parent information evenings about online safety every two years at least
- Delivering age-appropriate assemblies and workshops to children
- Rigorous implementation of the Online Safety Policy in both network design and use
- Use of safe and secure broadband with effective filtering.

Hazelwood ensures that the Online Safety Policy relates to other policies including those for behaviour, and safeguarding and child protection.

In writing these policies we will:

- Appoint an online safety Co-ordinator
- Ensure that the Online Safety Policy complies with all other policies on safeguarding children and has been agreed by senior leadership and approved by governors.
- Ensure that the Online Safety Policy is reviewed at least every three years

Managing Internet Access

3.1 Information system security

- ICT systems capacity and security will be reviewed regularly
- Virus protection will be updated regularly
- Varying rights of access depending on the role within school

3.2 Websites

3.2.1 Published content and the school website

- Website contact details include the school address, email and telephone number.
- Staff or children's personal information should not be published.
- Editorial responsibility lies with the member of staff designated by the Head

3.2.2 Publishing children's images and work

- During induction to the school, parents complete a form stating whether they grant the school permission to use children's photographs on the website and any publications.
- Children's full names should not be used anywhere on the website, particularly in association with photographs.
- When publishing children's work the school should seek permission of the child and parents.

3.2.3 Social networking and personal publishing

- The school should make arrangements to only allow access to social networking sites and Newsgroups, for specific supervised activities.
- Children should be advised never to give out personal details of any kind which may identify them or their location.

3.3 Video Conferencing

- All users should ask permission from the supervising member of staff before making or answering a video-conference call.
- Video-conferencing will be appropriately supervised for the children's age, and the School would ensure the quality and security of service used.

3.4 Internet filtering

- Hazelwood Schools ensures that appropriate filtering systems are in place when pupils and staff access school systems and internet provision. This is through London Grid for Learning (LGFL).
- The school will be careful to ensure that these systems do not place unreasonable restrictions on internet access or limit what children can be taught with regards to online teaching and safeguarding
- The systems should be reviewed and improved regularly.
- If an unsuitable site is discovered, it must be reported to the Online Safety Co-ordinator.

4. Emerging technologies

- Emerging technologies will be examined for educational benefit and an assessment of risks will be carried out before authorisation for use in school.

5. Personal data

- Personal data will always be recorded, processed, transferred and made available according to the Data Protection Act 1998.

6. Policy considerations

6.1 Authorising internet access

- All staff must read and sign the 'Acceptable ICT Use Agreement' before using any ICT resource. (Appendix iv)
- All staff and children are granted internet access which is regulated by LGFL.
- Parents will be asked to sign and return a consent form for internet access, as well as agreeing to responsible internet use by their child (Appendix ii)

6.2 Assessing risks

- We take all reasonable precautions to ensure that users access only appropriate material. However, due to the international scale and linked nature of internet content, it is not possible to guarantee that unsuitable material will never appear on a computer. Neither the school nor Enfield Council can accept liability for the material accessed, or any consequences of internet access.
- We audit ICT provision to establish if the Online Safety Policy is adequate and that its implementation is effective (Appendix iii).

6.3 Handling online safety complaints

- Complaints of internet misuse will be dealt with by a senior member of staff.
- Any complaint about staff misuse must be referred to the head/senior leader.
- Complaints of a child protection nature must be dealt with in accordance with child protection procedures.
- Children and parents will be informed of the complaints procedure.

7. Communications Policy

7.1 Introducing the Online Policy to children

- Online Safety rules will be posted in all networked rooms and discussed with children throughout the year (Appendix v)
- Children will be informed that network and internet use will be monitored
- Online Safety will be discussed through assemblies and curriculum

7.2 Staff Awareness

- All staff should be made aware of the importance of online safety and the associated policy
- Staff should exercise professional conduct when using the internet

- Staff should sign an Appropriate Use Agreement (Appendix iv)
- Staff are trained annually as part of their safeguarding children training

7.3 Parent Awareness

Parents/carers will be notified of online safety and associated policy via information evenings and the school website. Parents will also be made to sign an agreement that their child will comply with the online safety rules. (Appendix ii)

8. Online Safety Policy Audit

To ensure compliance and consistent implementation of online safety requirement we carry out an online safety audit (Appendix iii). For best results this should be initiated by a senior member of staff.

9. Useful Websites

- Childnet International: www.childnet.com
- UK Safer Internet Centre: www.saferinternet.org.uk
- Parents Info: www.parentsinfo.org
- Internet Matters: www.internetmater.org
- Net Aware: www.net-aware.org.uk
- ParentPort: www.parentport.org.uk
- Get safe Online: www.getsafeonline.org

Appendix i

Legal Framework

Obscene Publications Act 1959 and 1964

Publishing an 'obscene' article is a criminal offence. Publishing includes electronic transmission.

Protection of Children Act 1978 (section 1)

It is an offence to take, permit to be taken, make, possess, show, distribute or advertise indecent images of children in the United Kingdom. A child for these purposes is anyone under the age of 18. Viewing an indecent image of a child on your computer means that you have made a digital image. An image of a child also covers pseudo-photographs (digitally collated or otherwise). A person convicted of such an offence may face up to 10 years in prison.

Public Order Act 1986 (sections 17-29)

This act makes it a criminal offence to stir up racial hatred by displaying, publishing or distributing written material, which is threatening. Like the Racial and Religious Hatred Act 2006 it also makes the possession of inflammatory material with a view of releasing it a criminal offence.

Malicious Communications Act 1988 (section 1)

This legislation makes it a criminal offence to send an electronic message (email) that conveys indecent, grossly offensive, threatening material or information that is false; or is of an indecent or grossly offensive nature if the purpose was to cause a recipient to suffer distress or anxiety.

Copyright, Design and Patents Act 1988

Copyright is the right to prevent others from copying or using his or her 'work' without permission. The material to which copyright may attach (known in the business as 'work') must be the author's own creation and the result of some skill and judgement. It comes about when an individual expresses an idea in a tangible form. Works such as text, music, sound, film and programs all qualify for copyright protection. The author of the work is usually the copyright owner, but if it was created during the course of employment it belongs to the employer. It is an infringement of copyright to copy all or a substantial part of anyone's work without obtaining the author's permission. Usually a licence associated with the work will allow a user to copy or use it for limited 16 purposes. It is advisable always to read the terms of a licence before you copy or use someone else's material. It is also illegal to adapt or use software without a licence or in ways prohibited by the terms of the software licence

Data Protection Act 1998

The act requires anyone who handles personal information to notify the Information Commissioner's Office of the type of processing it administers, and must comply with important data protection principles when treating personal data relating to any living individual. The act also grants individuals rights of access to their personal data, compensation and prevention of processing.

The Computer Misuse Act 1990 (sections 1-3)

Regardless of an individual's motivation, the act makes it a criminal offence to:

- gain access to computer files or software without permission (for example using someone else's password to access files);
- gain unauthorised access, as above, in order to commit a further criminal act (such as fraud); or
- impair the operation of a computer or program (for example caused by viruses or denial of service attacks).

Protection from Harassment Act 1997

A person must not pursue a course of conduct, which amounts to harassment of another, and which he knows or ought to know amounts to harassment of the other. A person whose course of conduct causes another to fear, on at least two occasions, that violence will be used against him is guilty of an offence if he knows or ought to know that his course of conduct will cause the other so to fear on each of those occasions.

Regulation of Investigatory Powers Act 2000

The Regulation of Investigatory Powers Act 2000 (RIP) regulates the interception of communications and makes it an offence to intercept or monitor communications without the consent of the parties involved in the communication. The RIP was enacted to comply with the Human Rights Act 1998. The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, however, permit a degree of monitoring and record keeping, for example, to ensure communications are relevant to school activity or to investigate or detect unauthorised use of the network. Nevertheless, any monitoring is subject to informed consent, which means steps must have been taken to ensure that everyone who may use the system is informed that communications may be monitored. Covert monitoring without informing users that surveillance is taking place risks breaching data protection and privacy legislation.

Communications Act 2003 (section 127)

Sending by means of the internet a message or other matter that is grossly offensive or of an indecent, obscene or menacing character; or sending a false message by means of or persistently making use of the internet for the purpose of causing annoyance, inconvenience or needless anxiety is guilty of an offence liable, on conviction, to imprisonment. This wording is important because an offence is complete as soon as the message has been sent: there is no need to prove any intent or purpose.

The Counter-Terrorism and Security Act 2015

It was published on 12th March 2015. Section 26 of the Act places a duty on schools in England (and Wales) to prevent people being drawn into terrorism. This duty applies to all schools, whether publicly-funded or independent, and organisations covered by the Early Years Foundation Stage framework. Statutory guidance has been published and came into force on 1st July 2015.

www.legislation.gov.uk/ukdsi/2015/9780111133309/pdfs/ukdsiod_9780111133309_en.pdf

Appendix ii

Consent to Internet Access and Responsible Use

As part of your child's curriculum and the development of ICT skills and computing, Hazelwood Schools are providing

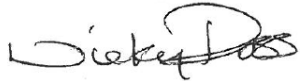
supervised access to the Internet. We believe that the use of the World Wide Web (WWW) and e-mail is worthwhile and is an essential skill for children as they grow up in the modern world. Please would you read the Rules for Responsible Internet Use and sign and return the consent form so that your child may use the Internet at school.

All our school computers are protected by the Enfield Borough filtering mechanism so that access on the Internet is limited to approved sites only. This may not be the case at home and we can provide references to information on safe Internet access if you wish.

Whilst every endeavour is made to ensure that suitable restrictions are in place for children to access inappropriate materials, Hazelwood Schools cannot be held responsible for the nature or content of materials accessed through the Internet. All internet access and computer use is supervised.

Should you wish to discuss any aspect of Internet use, please telephone the school to arrange an appointment to see either our ICT Technician or our Deputy Head.

Yours sincerely

A handwritten signature in black ink, appearing to read 'Nicky Ross', written in a cursive style.

Nicky Ross
Headteacher

HAZELWOOD SCHOOLS
Responsible Internet Use

We use the school computers and Internet connection for learning.
These rules will help us to be fair to others and keep everyone safe.

- ❖ I will ask permission before entering any web site, unless my teacher has already approved that site.
- ❖ I will not access the Internet without a teacher present.
- ❖ I will not look at or delete other people's files.
- ❖ I will not bring USB sticks into school without permission.
- ❖ I will only e-mail people I know, or those my teacher has approved.
- ❖ The messages I send will be polite and sensible.
- ❖ When sending e-mail, I will not give my home address or phone number, or arrange to meet someone.
- ❖ I will ask for permission before opening an e-mail or an e-mail attachment sent by someone I do not know.
- ❖ I will not use Internet chat or any other social media/messaging service without permission from my class teacher.
- ❖ If I see anything I am unhappy with or I receive messages I do not like, I will tell a teacher immediately.
- ❖ I know that the school may check my computer files and may monitor the Internet sites I visit.
- ❖ I understand that if I deliberately break these rules, I could be stopped from using the Internet, computers or any other devices.

The school may exercise its right by electronic means to monitor the use of the school computer system, including the monitoring of web sites, the interception of e-mail and the deletion of inappropriate materials in circumstances where it believes unauthorised use is, or may be taking place, or the system is or may be being used for criminal purposes or for the storing of text imagery which is unauthorised or unlawful.

Appendix iii

Online Safety Policy Audit

| Online Safety Requirement | Response | Outstanding Action |
|---|----------|--------------------|
| Has the school appointed an online safety coordinator? | | |
| When was the policy last updates/ refreshed? | | |
| Where can members of staff access a copy of the policy? | | |
| Where can parents access a copy of the policy? | | |
| Do parents sign and return an agreement that their child will comply with the online safety rules? | | |
| Who is the designated online safety coordinator? | | |
| Has online safety training been provided for both pupils and staff? | | |
| Have school online safety rules been set for pupils and displayed in the ICT suite? | | |
| Have all staff sign an Acceptable Use Agreement? | | |
| Is internet access provided by an approved educational internet service provider and complies with DCSF requirements? | | |
| Is personal data collected, stored and used according to the principles of the Data Protection Act? | | |
| Is this audit being initiated by a senior staff? | | |
| | | |
| Name of Staff carrying out the audit | | |
| Date of this audit | | |
| Date of subsequent audit | | |

Appendix iv

Staff ICT Acceptable Use Agreement

As a professional organisation with responsibility for children's safeguarding it is important that all staff take all possible and necessary measures to protect data and information systems from infection, unauthorised access, damage, loss, abuse and theft.

All members of staff have a responsibility to use the school's computer system in a professional, lawful, and ethical manner. To ensure that members of staff are fully aware of their professional responsibilities when using Information Communication Technology and the school systems, they are asked to read and sign this Acceptable Use Agreement.

This is not an exhaustive list and all members of staff are reminded that ICT use should be consistent with the school ethos, other appropriate policies and the Law.

- I understand that Information Systems and ICT include networks, data and data storage, online and offline communication technologies and access devices. Examples include mobile phones, PDAs, digital cameras, email and social media sites.
- School owned information systems must be used appropriately. I understand that the Computer Misuse Act 1990 makes the following criminal offences: to gain unauthorised access to computer material; to gain unauthorised access to computer material with intent to commit or facilitate commission of further offences or to modify computer material without authorisation.
- I understand that any hardware and software provided by my workplace for staff use can only be used by members of staff and only for educational use. To prevent unauthorised access to systems or personal data, I will not leave any information system unattended without first logging out or locking my login as appropriate.
- I will respect system security and I will not disclose any password or security information. I will use a 'strong' password.
- I will not attempt to install any purchased or downloaded software, including browser toolbars, or hardware without permission from the system manager.
- I will ensure that any personal data of pupils, staff or parents/carers is kept in accordance with the Data Protection Act 1988. Any images or videos of pupils will only be used as stated in the Online Safety Policy and will always take into account parental consent.
- I will not keep professional documents which contain school-related sensitive or personal information (including images, files, videos etc.) on any personal devices (such as laptops, digital cameras, mobile phones), unless they are secured and encrypted.
- I will protect the devices in my care from unapproved access or theft.
- I will not store any personal information on the school computer system that is unrelated to school activities, such as personal photographs, files or financial information.
- I will respect copyright and intellectual property rights.
- I have read and understood the school Online Safety Policy
- I will report all incidents of concern regarding children's online safety to the Designated Child Protection Coordinator and/or the Online Safety Coordinator as

soon as possible. I will report any accidental access, receipt of inappropriate materials, filtering breaches or unsuitable websites to the Online Safety Coordinator

- I will not attempt to bypass any filtering and/or security systems put in place by the school. If I suspect a computer or system has been damaged or affected by a virus or other malware or if I have lost any school related documents or files, then I will report this to the ICT Support Provider/Team as soon as possible.
- My electronic communications with pupils, parents/carers and other professionals will only take place via work approved communication channels e.g. via a school provided email address or telephone number. Any pre-existing relationships which may compromise this will be discussed with the Senior Leadership team.
- My use of ICT and information systems will always be compatible with my professional role, whether using school or personal systems. This includes the use of email, text, social media, social networking, gaming, web publications and any other devices or websites. My use of ICT will not interfere with my work duties and will be in accordance with the school policy and the Law.
- I will not create, transmit, display, publish or forward any material that is likely to harass, cause offence, inconvenience or needless anxiety to any other person, or anything which could bring my professional role, the school, or the Council, into disrepute.
- I will promote Online Safety with the pupils in my care and will help them to develop a responsible attitude to safety online, system use and to the content they access or create.
- If I have any queries or questions regarding safe and professional practise online either in school or off site, then I will raise them with the Online Safety Coordinator (name)
- I understand that my use of the information systems, Internet and email may be monitored and recorded to ensure policy compliance.

The School may exercise its right to monitor the use of information systems, including Internet access and the interception of e-mails in order to monitor compliance with this Acceptable Use Policy and the School's Data Security Policy. Where it believes unauthorised and/or inappropriate use of the service's information system or unacceptable or inappropriate behaviour may be taking place, the School will invoke its disciplinary procedure. If the School suspects that the system may be being used for criminal purposes or for storing unlawful text, imagery or sound, the matter will be brought to the attention of the relevant law enforcement organisation.

I have read and understood and agree to comply with the Staff ICT Acceptable Use Agreement.

Name: _____ Date: _____

Signed: _____

Appendix v

Pupil Understanding

I understand that I must use school ICT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the ICT systems and other users.

Keeping Safe

- I will not use ICT in school (including my own ICT) without permission
- I know that the school will monitor my use of the ICT systems and communications.
- I will only use my own user names and passwords which I will choose carefully to protect my identity and I will not share them.
- I will not ask computers to remember my password.
- I will keep my personal details and those of others private.
- I will log off sites and computers when finished.
- I understand that different sites have safety features and use them.
- I will not visit unsafe sites or register for things I am not old enough for.
- I will not try to upload, download or access anything online which is illegal or inappropriate or may cause harm or distress to others.
- I will not try to bypass the filtering and security systems in place on school ICT.

Communicating

- I know that I need to be polite and friendly online.
- I know that others may have different opinions and that I should respect them.
- I am careful about what I send in messages and the language I use as I know that messages can be forwarded on to my parents, head teacher or future employer.
- I know that people online may not be who they seem.
- I will make sure my teacher / parents know who I communicate with online.
- If I want to arrange to meet an online friend I will tell an adult and take someone with me.
- I will not open messages if the subject field contains anything offensive or if I do not know who it is from.
- I will only use chat and social networking sites that the school allows.

Research and Fun

- I will use clear search words so that I can find the information I want safely.
- I will double check the information that I find, as some information online may not be truthful.
- I know that some content may not be filtered out.
- I know that school ICT is for learning and I will not use the systems for personal use or fun unless I have permission. This includes making large downloads/uploads, games, shopping and video broadcasting.

Sharing

- I will not access or use any other user's files without their permission and will credit their work if I use it.
- Where work is protected by copyright, I will not try to download copies (including music and videos).
- I know that downloading from file shares is illegal and that it can lead to viruses which could damage the computer, slow it down and eventually lead to it having to be removed and cleaned.

- I know that there are proposals to actively pursue piracy by monitoring file share sites to see who is downloading and then tracing the user through the ISP.
- I will not take or share images of anyone without their permission.
- I will take care about what I publish on the web as I know once published I cannot control what it is used for.

Buying and selling

- I know that I should ask permission if I am buying / selling anything online.
- I know that I should not respond to offers that I have not asked for as they may be scams.
- I will not use someone else's identity to buy things online

Problems

- I will not try to alter computer settings or install programmes unless I have permission.
- I will immediately report any unpleasant or inappropriate material or messages that I see on computer or online.
- I will not damage equipment and will report any damage or faults involving equipment or software, however this may have happened.
- If I receive an upsetting message / e-mail I will not reply but will save it and report it. If it is received via a chat program or posted on a social networking site, I know I should take a screen shot of it so it can clearly be seen in context.
- I know that viruses and other harmful programmes can be sent by e-mail so I will not open any attachments to emails unless I know and trust the person who sent it.

Appendix vi

How to deal with infringements

Students

Deliberate infringements

- Deliberately corrupting or destroying someone's data, violating privacy of others or posts inappropriate messages, videos or images on a social networking site.
- Sending an email or MSN message that is regarded as harassment or of a bullying nature (one-off)
- Trying to access offensive or pornographic material (one-off)
- Purchasing or ordering of items online
- Transmission of commercial or advertising material

Persistent deliberate infringements

- Continued sending of emails or MSN messages regarded as harassment or of a bullying nature after being warned
- Deliberately creating, accessing, downloading or disseminating any material deemed offensive, obscene, defamatory, racist, homophobic or violent
- Receipt or transmission of material that infringes the copyright of another person or infringes the conditions of the Data Protection Act, revised 1988
- Bringing the school name into disrepute

Staff

Misconduct

- Excessive use of Internet for personal activities not related to professional development e.g. online shopping, personal email, instant messaging etc.
- Use of personal data storage media (e.g. USB memory sticks) without considering access and appropriateness of any files stored.
- Not implementing appropriate safeguarding procedures.
- Any behaviour on the World Wide Web that compromises the staff members professional standing in the school and community.
- Misuse of first level data security, e.g. wrongful use of passwords.
- Breaching copyright or license e.g. installing unlicensed software on network.

Gross misconduct

- Serious misuse of, or deliberate damage to, any school / Council computer hardware or software;
- Any deliberate attempt to breach data protection or computer security rules;
- Deliberately creating, accessing, downloading and disseminating any material deemed offensive, obscene, defamatory, racist, homophobic or violent;
- Receipt or transmission of material that infringes the copyright of another person or infringes the conditions of the Data Protection Act, revised 1988;
- Bringing the school name into disrepute