E-SAFETY POLICY

1. Introduction

In the last 25 years, the world has been revolutionised by information technology in general, and social media and mobile technology in particular. Children currently at school know no other world than one of instant connectivity. The potential benefits to them individually and to society as a whole are enormous. Indeed, IT competence must be regarded an absolutely essential skill for all children, for future further and higher education opportunities and employment, as well as socially. However, despite an overall picture of positive progress, the internet is not wholly unproblematic. In addition to specific safety risks (such as online 'grooming'), other potential risks include easy and unfettered access to adult-orientated material (such as pornography and online gambling), misleading and manipulative material (fake news), Social Media bullying, the 'addictive' quality of some online activities, along with the research indicating the negative effect of excessive screen time on both healthy brain development, physical activity and 'real-life' social interaction.

This e-Safety Policy encompasses internet technologies and electronic communications such as smart phones, wireless technology as well as collaboration tools and personal publishing. It highlights the need to educate pupils about the benefits and risks of using technology and provides safeguards and awareness for users to enable them to control their online experiences.

The previous Internet Policy has been revised and renamed as the School's e-Safety Policy to reflect the need to raise awareness of the safety issues associated with electronic communications as a whole.

The school's e-Safety Policy operates in conjunction with other policies including Behaviour for Learning, Prevention of Bullying, Curriculum, Data Protection and Security and Safeguarding Policies.

End-to-end e-Safety depends on effective practice at a number of levels:

- Responsible ICT use by all staff and pupils; encouraged by education and made explicit through published policies.
- Sound implementation of e-Safety Policy in both administration and curriculum, including secure school network design and use.
- National Education Network standards and specifications.

2. Writing & Reviewing the e-Safety Policy

This e-Safety Policy relates to other policies including those for Prevention of Bullying and Safeguarding. The school e-Safety Policy has been written in line with government guidance and has built upon a recommended e-Safety Policy. This e-Safety Policy and its implementation will be reviewed every 24-months.

3. Teaching & Learning

Why Internet Use is Important

- The Internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide students with quality Internet access as part of their learning experience
- Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils. **Internet use enhances learning**

- The school Internet access will be designed expressly for pupil use and will include filtering appropriate to the age of pupils
- Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation

Pupils Are Taught How to Evaluate Internet Content

- The school will ensure that the use of Internet derived materials by staff and pupils complies with copyright law.
- Pupils should be taught to be critically aware of the materials they read, and shown how to validate information before accepting its accuracy

4. Managing Internet Access

Information system security:

- School ICT systems capacity and security will be reviewed regularly.
- Virus protection will be updated regularly.
- Security strategies will be discussed with mainstream schools

5. E-mail

Pupils may NOT use e-mail accounts on the school system, other than those set up by the school to teach them to use email safely (and then only within the control of the teacher delivering the lessons).

6. Published Content & the School Website

The contact details on the Web site should be the school address, e-mail and telephone number. Staff or pupils' personal information will not be published. Overall responsibility for the website that of the Headteacher.

7. Publishing Pupil's Images & Work

Photographs that include pupils where they can be easily identified will NOT be used on the internet. Pupils' names will not be used anywhere on the website. Written permission from parents or carers will be obtained before photographs of pupils are published on the school website. All material for publication on the web must have been approved by the Headteacher.

8. Social Networking & Personal Publishing

For the reasons of pupil safety, Hartmore School blocks does not allow access to social networking sites (e.g. Instagram, Facebook, Twitter, tik tok). Pupils are advised never to reveal personal details of any kind, which may identify them or their location.

Pupils and parents will be advised that the use of Social Networks outside school should be limited only to age-appropriate groups; and then only if carefully monitored and controlled.

No member of staff may privately 'friend' or 'follow' a pupil on any Social Network site.

9. Managing Filtering

Our experience is that no filtering system is sufficient to keep children safe on the internet. Rather than rely on a filtering system to keep children safe (which can leads to complacency), the responsibility rests with the staff to ensure children are using the internet safely and appropriately at all times. To this end staff maintain we have a simple rule "No Screen Unseen" by an adult. Staff maintain 100% supervision i.e. if a pupil is using the internet, then the supervising adult can ensure what they are accessing is appropriate. If it is not they will immediately intervene, closing down inappropriate material.

The Internet Service Provider's to systems to protect pupils are regularly reviewed and improved. If staff or pupils discover an unsuitable site, it must be reported to the Headteacher. The Headteacher will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

10. 'Smart Phones' & Other Mobile Electronic Devices

Many, if not most pupils now have access to a smart phone, iPad, android device, kindle or similar. Unless carefully managed, these technologies allow pupils to browse any part of the internet without effective supervision or adult oversight. This has implications in terms of pupils viewing adult- orientated material, being a significant distraction to learning and in offering temptations to 'cheat'. As such, Pupils are strictly prohibited from bringing mobile/smart phones (or other similar devices) to school.

If any pupil needs to contact parents/carers etc. in an emergency during the school day, the School Office telephone system to contact. Similarly, parents and carers can contact their child in the same way. They can also email the School Secretary, who will pass on any message.

Staff should not use their personal mobile phone, personal email address etc. to contact pupils or their parents/carers.

11. Policy Decisions

Assessing risks

Hartmore School takes all reasonable precautions to ensure that users access only appropriate material. However, due to the sheer scale and amount of Internet content (and the ease with which it can accessed), it is simply not possible to guarantee that unsuitable material will never appear on a school computer. Nevertheless, 100 % supervision of internet access is maintained i.e. if a pupil is browsing the net, then an adult is always closely supervising them. The adult immediately intervenes and cease any activity which is inappropriate. NB: The School cannot accept liability for the material accessed, or any consequences of Internet access.

The school regularly audits its ICT provision to establish if the e-safety Policy is adequate, and that its implementation is effective. This is particularly important in the area of e-Safety, as everchanging technology can easy outpace the provisions of this Policy.

Handling e-safety Complaints

Complaints regarding Internet misuse are always dealt with by a senior member of staff. Any complaints regarding staff misuse must be referred to the Headteacher.

Complaints of a child protection nature must be dealt with in accordance with school child protection procedures and Safeguarding Policy. Pupils and parents will be informed of the complaints procedure.

The Police Youth Crime Reduction Officer is consulted regularly to inform procedures for handling potentially illegal issues.

Community Use of the Internet

School staff will be responsible for the actions of any adult guests or visitors who they allow to use the school internet facilities. Their attention will be drawn to the School's policy and the e-safety rules.

The school will liaise with local organisations as appropriate to establish a common approach to e-safety.

12. Communications Policy

Introducing the e-safety Policy to Pupils

E-safety rules will be posted in all networked rooms and discussed with the pupils at the start of each year. Pupils will be informed that network and Internet use will be monitored.

Staff & the e-Safety Policy

All staff must read the School e-Safety Policy, and recognise its importance.

Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential. Staff that manage filtering systems or monitor ICT are supervised by senior management, and have clear procedures for reporting issues.

Enlisting Parents' Support

Parents' attention is drawn to the School e-Safety Policy. They will be notified as to any concerns the School has about their child's internet safety. The School works closely with parents to help ensure children are safe on the internet both in school and at home.

Policy Review

This Policy was last reviewed in October 2020. The next reviewed is due in September 2022. The School regularly audits its ICT provision to ensure that this e-safety Policy remains adequate and up-to- date, and that its implementation is effective. This is particularly important in this area, as ever- changing technology can easy outpace the provisions of this Policy.

Appendix I

Internet Use - Possible Teaching & Learning Activities

Activities	Key e-safety issues	Relevant Websites
Creating web directories to provide easy access to suitable websites.	Pupils should be supervised. Pupils should be directed to specific, approved on-line materials.	Web directories e.g. Ikeep bookmarks Webquest UK
Using search engines to access information from a range of websites.	Parental consent should be sought. Pupils should be supervised. Pupils should be taught what internet use is acceptable and what to do if they access material they are uncomfortable with.	Web quests e.g. - Google - Ask Jeeves for kids - Yahooligans - CBBC Search - Kidsclick - BBC Bitesize
Publishing pupils' work on school and other websites.	Pupil and parental consent should be sought prior to publication. Pupils' full names and other personal information should be omitted.	Making the News SuperClubs Infomapper Headline History Focus on Film
Publishing images including photographs of pupils.	Parental consent for publication of photographs should be sought. Photographs should not enable individual pupils to be identified. File names should not refer to the pupil by name.	Making the News SuperClubs Learninggrids Museum sites, etc. Digital Storytelling BBC – Primary Art

Appendix II

Procedures to be followed:

In the event of pupils being exposed to undesirable materials.

- The pupils should know to notify a teacher immediately; e-safety rules are displayed in all classrooms with computer and internet access
- The Headteacher will be notified by the teacher as soon as reasonably practicable
- Parents/carers will be notified according to the degree of seriousness of the incident (for example, exposure to materials that include common profanities might not be notified to parents but exposure to materials that included pornographic images would).

In the event of pupils intentionally accessing undesirable materials.

- All pupils will be made well aware of the seriousness of intentionally accessing undesirable materials on the internet in school. The child parents/carers will be informed in handover. Further advice sought by the school as necessary.

- If deliberate access to undesirable materials is found to be repeated by a pupil or pupils then the matter will be treated very seriously and the pupils parents/carers will again be informed and notified with decisions re actions to be taken.

In the event of adults intentionally accessing undesirable materials.

- Deliberate access by any adult to unacceptable material in school will be treated as a disciplinary matter. The Headteacher or Directors will be made aware immediately.

Appendix III

Definitions

Undesirable Materials

- Pornographic images or obscene texts on internet websites, social media or mobile/smart phones
- Any violent images or content
- Language that is abusive, profane, inflammatory, coercive, defamatory, blasphemous or otherwise offensive on websites, social media, text messaging or emails
- Racist, exploitive or illegal materials or messages on websites, social media, mobile/smart phones or emails

Undesirable Contacts

- Email messages or text messages from unknown or unverified parties who seek to establish a pupil's identity and/ or communicate with them

Unacceptable Use

- Deliberate searching for, and accessing, of undesirable materials
- Creating and transmitting emails, text messages or social media posts that contain unacceptable language or content

Adults

- All staff
- Visitors and guests
- Directors
- Parents/ and or governors
- Volunteers in school
- Students on work experience placements

Appendix IV

Internet facilities in School

General Points

- The school has five classrooms with multiple Laptops in each classroom, all linked to the internet. There is a white board in every classroom to support teaching and learning
- All classrooms have internet access. Teachers have responsibility for ensuring appropriate usage of these connections at all times
- All staff can use the internet facility outside school hours to support them in their work
- All staff are provided with a school email account

However, before using the facility it is vitally important that:

- All staff have read the e-safety policy and the guidelines laid down within it
- All pupils are aware of the e-safety rules
- All users have the necessary skills to use the facility safely and for the intended purpose

N.B. Support with developing ICT skills can be provided through CP

Appendix V

e-Safety Rules

Key Stage 1 and 2

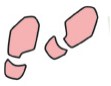
Think then Click

These rules help us to stay safe on the Internet

We only use the internet when an adult is with us

We can click on the buttons or links when we know what they do.

We can search the Internet with an adult.



We always ask if we get lost on the Internet.

e-Safety Rules

Key Stage 3 & 4

Think Then Click
e-Safety Rules for Key Stage 3 and 4
• We ask permission before using the Internet • We only use websites that an adult has chosen • We tell an adult if we see anything we are uncomfortable with • We immediately close any web-page we not sure about • We never give out personal information or passwords • We never arrange to meet anyone we don't know • We do not use Internet chat rooms

These e-Safety Rules help to protect pupils and the school by describing acceptable and unacceptable computer use.

- The school owns the computer network and can set rules for its use
- It is a criminal offence to use a computer or network for a purpose not permitted by the school
- Irresponsible use may result in the loss of network or Internet access
- Network access must be made via the user's authorised account and password, which must not be given to any other person.
- All network and Internet use must be appropriate to education
- Copyright and intellectual property rights must be respected
- Messages shall be written carefully and politely, particularly as email could be forwarded to unintended readers
- Anonymous messages and chain letters are not permitted.
- Users must take care not to reveal personal information through email, personal publishing, blogs or messaging
- The school ICT systems may not be used for private purposes, unless the head teacher has given specific permission
- Use for personal financial gain, gambling, political activity, advertising or illegal purposes is not permitted

Hartmore School may exercise its right to monitor the use of its computer systems, including access to websites, social media, the interception of e-mail and the deletion of inappropriate materials where it believes unauthorised use of the school's computer system may be taking place, or the system may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound

Appendix VI

Smile & Stay Safe Poster

AND STAY SAFE

Staying safe means keeping your personal details private, such as full name, phone number, home address, photos or school. Never reply to ASL (age, sex, location).

Meeting up with someone you have met online can be dangerous. Only meet up if you have first told your parent or carer and they can be with you.

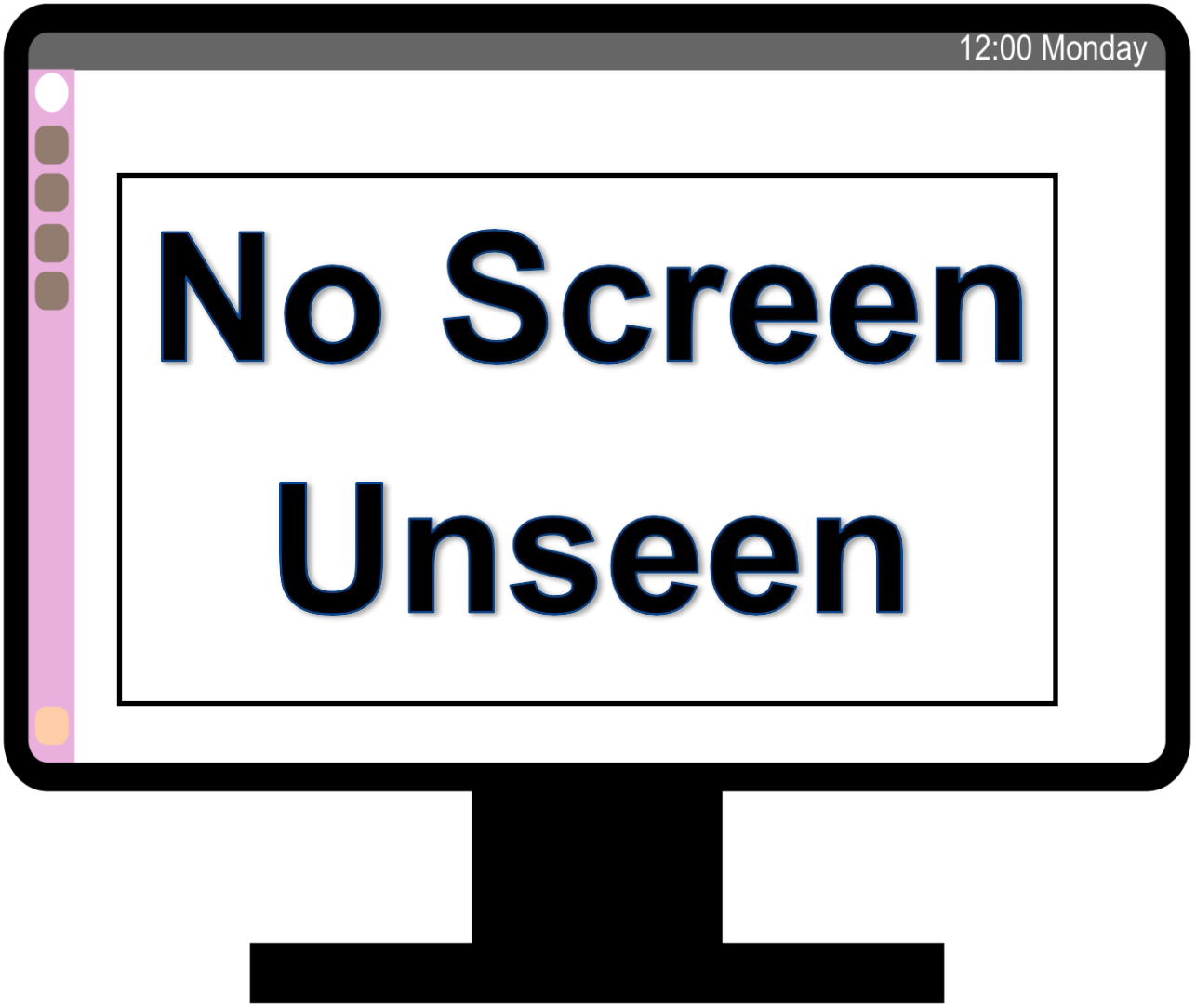
Information online can be untrue, biased or just inaccurate. Someone online my not be telling the truth about who they are - they may not be a 'friend'.

Let a parent, carer, teacher or trusted adult know if you ever feel worried, uncomfortable or frightened about something online or someone you have met or who has contacted you online.

Emails, downloads, IM messages, photos and anything from someone you do not know or trust may contain a virus or unpleasant message. So do not open or reply.

Appendix VII

No Screen Unseen Poster



Appendix VIII

Legislation

Acts Relating to the Monitoring of Staff Email

Data Protection Act 1998
The Act requires anyone who handles personal information to comply with important data protection principles when treating personal data relating to any living individual. The Act grants individuals rights of access to their personal data, compensation and prevention of processing.
http://www.hmso.gov.uk/acts/acts1998/19980029.htm

The Telecommunications (Lawful Business Practice)
(Interception of Communications) Regulations 2000
http://www.hmso.gov.uk/si/si2000/20002699.htm

Regulation of Investigatory Powers Act 2000
Regulating the interception of communications and making 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.
http://www.hmso.gov.uk/acts/acts2000/20000023.htm

Human Rights Act 1998
http://www.hmso.gov.uk/acts/acts1998/19980042.htm

Other Acts relating to e-Safety

Racial and Religious Hatred Act 2006
It a criminal offence to threaten people because of their faith, or to stir up religious hatred by displaying, publishing or distributing written material which is threatening. Other laws already protect people from threats based on their race, nationality or ethnic background.

Sexual Offences Act 2003
The new grooming offence is committed if you are over 18 and have communicated with a child under 16 at least twice (including by phone or using the Internet) it is an offence to meet them or travel to meet them anywhere in the world with the intention of committing a sexual offence. Causing a child under 16 to watch a sexual act is illegal, including looking at images such as videos, photos or webcams, for your own gratification. It is also an offence for a person in a position of trust to engage in sexual activity with any person under 18, with whom they are in a position of trust. Schools should already have a copy of "*Children & Families: Safer from Sexual Crime*" document as part of their child protection packs.
For more information
www.teachernet.gov.uk

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 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 another person's password to access files)
- Unauthorised access, as above, in order to commit a further criminal act (such as fraud)
- Impair the operation of a computer or program
- UK citizens or residents may be extradited to another country if they are suspected of committing any of the above offences

Malicious Communications Act 1988 (section 1)
This legislation makes it a criminal offence to send an electronic message (e-mail) 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 & Patents Act 1988
Copyright is the right to prevent others from copying or using work without permission. 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. Copyright infringement is to copy all or a substantial part of anyone's work without obtaining them author's permission. Usually a licence associated with the work will allow a user to copy or use it for limited 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.

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.

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 a 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.

Obscene Publications Act 1959 and 1964
Publishing an "obscene" article is a criminal offence. Publishing includes electronic transmission.

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.