



The Hampshire School
C H E L S E A

The Hampshire School Online Safety Policy

Early Years, Pre-Preparatory and Preparatory comply with this Policy and Guidance

Next review Date: September 2019

Reviewed: Miss Bagaric (Head of ICT)/ Miss Reddaway (DSL) February 2019

Contents

1. Introduction
2. Appropriate strategies
3. Pupils understanding of how to keep safe online
4. Pupils' evaluation of Internet content
5. Management of email
6. Management of website content
7. Newsgroups and chat
8. Management of emerging Internet uses
9. Authorisation of Internet access
10. Liaison and partnership with parents
11. Assessing the risks of Internet Use and Management of filtering
12. Introduction of the policy to pupils
13. Staff consultation and training
14. Technical provision, filters, safeguards and monitoring
15. Maintenance of ICT system security
16. Appendix 1 ONLINE SAFETY CONTRACT
17. Appendix 2 ACCEPTABLE USE AGREEMENT (STAFF, VOLUNTEERS AND VISITORS)
18. Appendix 3 ONLINE SAFETY TRAINING NEEDS – SELF-AUDIT FOR STAFF
19. Appendix 4 ONLINE SAFETY INCIDENT REPORT LOG

1. Introduction

The Hampshire School believes in the educational benefits of curriculum Internet use. Good planning and management that recognises the risks will help to ensure appropriate, effective and safe pupil use. In delivering the curriculum, teachers plan the integration and use of communications technology such as web-based resources and e-mail in order to enable pupils to learn how to locate, retrieve and exchange information using ICT. Computer skills are vital to access life-long learning and for future employment. Most technologies present risks as well as benefits. Internet use for home, social and leisure activities is expanding and being used by all sectors of society. This brings young people into contact with a wide variety of influences, some of which could be unsuitable. It is important that schools, as well as parents, adopt strategies for the responsible and safe use of the Internet.

Core Principles of Internet Safety

The Internet has become as commonplace as the mobile phone or TV and its effective use is an essential life-skill. Unmediated Internet access brings with it the possibility placing of pupils in embarrassing, inappropriate and even dangerous situations. This policy aims to help to ensure responsible use and the safety of pupils.

Guided educational use

Significant educational benefits should result from curriculum Internet use including access to information from around the world and the ability to communicate widely and to publish easily. Internet use should be planned, task-orientated and educational within a regulated and managed environment. Directed and successful Internet use will also reduce the opportunities for activities of dubious worth.

Risk assessment

21st Century life presents dangers including violence, racism and exploitation from which children and young people need to be protected. At the same time they need to learn to recognise and avoid these risks – to become “Internet Wise”. Pupils need to know how to cope if they come across inappropriate material.

Responsibility

Internet safety depends on staff, schools, governors, advisers, parents and, where appropriate, the pupils themselves taking responsibility for the use of Internet and associated communication technologies. The balance between education for responsible use, regulation and technical solutions must be judged carefully. It is acknowledged that, whilst the school provides pupils with a protected environment for Internet usage in school, the pupils may not benefit from the same level of protection in their access to the Internet beyond the confines of the school. Important aspects of the school’s online provision are, therefore, the development of the pupils’ understanding of keeping safe online when not at school, and supporting parents in understanding how to help keep their children safe online.

- The Head is responsible for ensuring, so far as is reasonably practicable, a safe environment for internet use, for the implementation of policy and for the development of the pupils’ understanding of how to keep themselves safe online, both in and out of school.
- The ICT Manager is responsible for the maintenance of hardware and software systems and technology to ensure, so far as is reasonably practical, safe use of the internet.
- The ICT Co-ordinator is responsible for overseeing the successful development, both in ICT lesson and the wider curriculum and extra-curricular activities, of pupils’ understanding of how to keep safe online and for supporting staff in implementing this objective.
- All staff and volunteers are responsible for monitoring pupils’ safety online and reporting any concerns arising from pupils’ internet use, either at school or at home, and for supporting the development of the pupils’ understanding of how to keep themselves safe online.

Regulation

The use of a limited and expensive resource, which brings with it the possibility of misuse, must be regulated. In some cases, access within school is denied, for instance unmoderated chat rooms present immediate dangers and are banned. Fair rules, clarified by discussion and prominently displayed help pupils make responsible decisions for both school and home access.

2. Appropriate strategies

This document describes strategies to help to ensure responsible and safe use. They are based on limiting access, developing responsibility and on guiding pupils towards educational activities.

There are no straightforward or totally effective solutions and staff, parents and the pupils themselves must remain vigilant.

a) The Importance of Internet Use

- The purpose of Internet use in school is to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the school's management information and business administration systems.
- Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils.
- The Internet is an essential element in 21st Century life for education, business and interaction. The school has a duty to provide students with quality Internet access as part of their learning experience.

b) How the Internet benefits education

Benefits of using the Internet in education include:

- access to world-wide educational resources including museums and art galleries;
- educational and cultural exchanges between pupils world-wide;
- cultural, vocational, social and leisure use in libraries, clubs and at home;
- access to experts in many fields for pupils and staff;
- staff professional development through access to national developments, educational materials and good curriculum practice;
- communication with support services, professional associations and colleagues;
- improved access to technical support including remote management of networks.

c) How Internet use enhances learning

- The school Internet access is designed expressly for pupil use and will include filtering appropriate to the age of pupils.
- Pupils will be taught what is acceptable and what is not acceptable and given clear objectives for Internet use.
- Internet access will be planned to enrich and extend learning activities. Access levels will be reviewed to reflect the curriculum requirements and age of pupils.
- Staff will guide pupils in on-line activities that will support the learning outcomes planned for the pupils' age and maturity.
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location and retrieval.

3) Pupil's Understanding of how to keep safe online

The school develops the pupils' understanding of how to keep safe online, as part of a broad and balanced curriculum, and their resilience in protecting themselves and their peers in the following ways:

In Key Stage 1, pupils will be taught to:

- Use technology safely and respectfully, keeping personal information private

- Identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies

Pupils in Key Stage 2 will be taught to:

- Use technology safely, respectfully and responsibly
- Recognise acceptable and unacceptable behaviour
- Identify a range of ways to report concerns about content and contact

In Key Stage 3, pupils will be taught to:

- Understand a range of ways to use technology safely, respectfully, responsibly, critically and securely, including protecting their online identity and privacy
- Recognise inappropriate content, contact and conduct, and know how to report concerns

The safe use of social media and the internet will also be covered in other subjects where relevant. The school will use assemblies, form time and PSHE lessons to raise pupils' awareness.

4) Pupils' Evaluation of Internet content

Inappropriate material should not be visible to pupils using the Web. This is not easy to achieve and cannot be guaranteed. It is a sad fact that pupils may be confronted with inappropriate material, despite all attempts at filtering. Pupils will be taught what to do if they experience material that they find distasteful, uncomfortable or threatening. For example, to close the page and report the URL to the teacher or ICT manager for inclusion in the list of blocked sites. More often, pupils will be judging reasonable material but selecting that which is relevant to their needs, for instance to answer a homework question. Pupils should be taught research techniques including the use of subject catalogues and search engines. They will be encouraged to question the validity, currency and origins of information – key information handling skills. They should also use alternative sources of information for comparison purposes. Effective guided use will reduce the opportunity pupils have for exploring unsavoury areas. Using Internet derived materials in pupils' own work requires at least an understanding that straight copying is worth little without a commentary that demonstrates the selectivity used and evaluates significance. Respect for copyright and intellectual property rights, and the correct usage of published material needs to be taught.

If staff or pupils discover unsuitable sites, the URL (address) and content must be reported to the Internet Service Provider via the ICT co-ordinator.

- The use of Internet derived materials by staff and by pupils in school must comply with copyright law.
- Pupils are taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- Pupils will be taught to acknowledge the source of information and to respect copyright when using Internet material in their own work.

5) Management of e-mail

- Pupils may use only approved e-mail accounts on the school system.
- Pupils must immediately tell a teacher if they receive offensive e-mail.
- Pupils must not reveal details of themselves or others, such as address or telephone number, or arrange to meet anyone in e-mail communication.
- Access in school to external personal e-mail accounts is not allowed except where a teacher has specifically requested it for example to retrieve a piece of work emailed from home.

6) Management of Website content

- The point of contact on the Website is the school address/school e-mail and telephone number. □ Staff or pupils' home information will not be published.

- Website photographs that include pupils will be selected carefully and will not enable individual pupils to be identified.
- Pupils' full names will not be used anywhere on the Website, particularly associated with photographs.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school Website.
- The copyright of all material must be held by the school, or be attributed to the owner where permission to reproduce has been obtained.
- The school undertakes appropriate measures for the management of personal data which is stored electronically.

□

7) Newsgroups and chat

- Pupils will not be allowed access to public or unregulated chat rooms in school.
- Newsgroups will not be made available unless an educational requirement for their use has been demonstrated.
- A risk assessment will be carried out before pupils are allowed to use a new technology in school.

8) Management of emerging Internet uses

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.

9) Authorisation for Internet access

- At EYFS and Key Stage 1, access to the Internet will be by adult demonstration and with directly supervised access to specific, approved on-line materials.

10) Liaison and partnership with parents

Parents have access to the school's e-safety policy on the school website and can request a paper copy from the school office.

- Parents will be informed that pupils will be provided with supervised Internet access.
- Parents and pupils will be asked to sign and return a consent form.
- Periodically the school runs e-safety information meetings for parents, which may involve an external speaker, in order to raise their awareness of e-safety matters and help them develop their children's safe use of the Internet.
- Copies of template agreements for children and parents are found in Appendix 1 of this policy.

11) Assessing the risks of Internet Use and Management of filtering

- In common with other media such as magazines, books and video, some material available via the Internet is unsuitable for pupils. The school will 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 school computer.
- Methods to identify, assess and minimise risks will be reviewed regularly.
- The Head teacher will ensure that the Internet policy is implemented and compliance with the policy monitored.

- The school will work in partnership with parents, the DfE and our Internet Service Provider to ensure systems to protect pupils are reviewed and improved.
- The school will ensure that appropriate IT filters and monitoring procedures are in place to safeguard children from potentially harmful and inappropriate material online without unreasonable 'overblocking'.
- We do not allow pupils to have mobile phones in school. Prep School pupils may leave a mobile phone at Reception each morning for collection at the end of day, if required.

12) Introduction of the policy to pupils

- Rules for Internet access will be posted near all computer systems.
- Pupils will be informed that Internet use will be monitored.
- Instruction in responsible and safe use should precede Internet access.

13) Staff consultation and training

- The school will ensure that all staff have undertaken appropriate online safety training
- All staff must have familiarised themselves fully with this policy before using any Internet resource in school.
- All staff, including teachers, supply staff, classroom assistants and support staff, will be provided with the School Internet Policy, and its importance explained.
- Staff development in the safe and responsible Internet use, and on school Internet policy will be provided as required. Induction training in safeguarding for new staff includes online safety.
- The school uses Educare and in-house training for online safety.

14) Technical provision, filters, safeguards and monitoring The ICT manager is responsible for:

- Putting in place appropriate filtering and monitoring systems, which are updated on a regular basis and keep pupils safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material
- Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Conducting a full security check and monitoring the school's ICT systems on a regular basis

Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files:

- Ensuring that any online safety incidents are logged (see appendix 4) and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy

This list is not intended to be exhaustive

16) Maintenance of ICT system security

- The school ICT systems will be reviewed regularly with regard to security in conjunction with the School's ICT Manager.
- Virus protection will be installed and updated regularly by the ICT Manager.
- Memory sticks and other such portable storage devices may be brought into school when specific permission has been given.
- Unapproved system utilities and executable files will not be allowed in pupils' work areas or attached to e-mail.

Online safety contract (Please complete, sign and return to your class teacher)			
Pupil's Agreement I have read and I understand the pupil's online safety agreement, and will abide by the rules which are designed to keep both myself and the school safe.			
Name:	Class:	Signed:	Date:
Parent's Consent/Agreement I have read and understood the online safety agreement and give permission for my son / daughter to access the Internet at school, and will encourage them to abide by these rules. Children will receive advice on online safety at school. Advice for parents is available at https://www.nspcc.org.uk/preventing-abuse/keeping-children-safe/online-safety/ or by contacting the school. I understand that the school will take reasonable precautions to ensure pupils cannot access inappropriate materials. However, due to the scale of the internet content, it is not possible to guarantee that unsuitable materials will never appear on a school computer. Neither the school nor GEMS can accept liability for the material or any consequences of internet access. I will encourage my child to adopt safe use of the internet and digital technologies at home and will inform the school if I have concerns over my child's e-safety. I will ensure that any pictures and/or videos taken, or purchased, during school events that include other children, will not be shared using social media. I will not post anything inappropriate on social media about the school, staff or other children (i.e. facebook, whatsapp, twitter etc...)			
I give permission for the school to use digital images and videos of my child and for their work to be displayed in the following ways:			
Displays around the school	YES <input type="checkbox"/>	NO <input type="checkbox"/>	
Newsletters	YES <input type="checkbox"/>	NO <input type="checkbox"/>	
School website	YES <input type="checkbox"/>	NO <input type="checkbox"/>	
Prospectus	YES <input type="checkbox"/>	NO <input type="checkbox"/>	
Social Media	YES <input type="checkbox"/>	NO <input type="checkbox"/>	
Signed:		Date:	
Please print name			

APPENDIX 2: ACCEPTABLE USE AGREEMENT (STAFF, VOLUNTEERS AND VISITORS)

Acceptable use of the school's ICT systems and the internet: agreement for staff, volunteers and visitors

Name of staff member/volunteer/visitor:

When using the school's ICT systems or personal equipment in school (to include accessing the internet) or outside school on a work device, I will not:

- Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature
- Use them in any way which could harm the school's reputation
- Access social networking sites or chat rooms
- Use any improper language when communicating online, including in emails or other messaging services
- Install any unauthorised software
- Share my password with others or log in to the school's network using someone else's details

I will only use the school's ICT systems and access the internet in school, or outside school on a work device, for educational purposes or for the purpose of fulfilling the duties of my role. This includes the usage of personal equipment within school.

I agree that the school will monitor the websites I visit.

I will take all reasonable steps to ensure that work devices are secure and password protected when using them outside school, and keep all data securely stored in accordance with this policy and the school's data protection policy.

I will let the designated safeguarding lead (DSL) and ICT manager know if a pupil informs me they have found any material which might upset, distress or harm them or others, and will also do so if I encounter any such material.

I will always use the school's ICT systems and internet responsibly, and ensure that pupils in my care do so too.

Signed (staff member/volunteer/visitor):

Date:

APPENDIX 3: ONLINE SAFETY TRAINING NEEDS – SELF-AUDIT FOR STAFF

Online safety training needs audit	
Name of staff member/volunteer:	Date:
Do you know the name of the person who has lead responsibility for online safety in school?	
Do you know what you must do if a pupil approaches you with a concern or issue?	
Are you familiar with the school's acceptable use agreement for staff, volunteers, governors and visitors?	
Are you familiar with the school's acceptable use agreement for pupils and parents?	
Are you familiar with the school's approach to tackling cyberbullying?	

<p>Are there any areas of online safety in which you would like training/further training? Please record them here.</p>	
-----------------------------------------------------------------------------------------------------------------------------	--

The Hampshire School Chelsea Staff
Online Safety Policy

APPENDIX 4: ONLINE SAFETY INCIDENT REPORT LOG

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

--	--	--	--	--

Reviewed: Miss Bagaric (Head of ICT) February 2019