E-Safety Policy

Ashley Junior School

Approved by:	Curriculum, Standards & Welfare Committee	**Date:**	11.01.2019
Last reviewed on:	20.1.2021		
Next review due by:	January 2022		

Ashley Junior School
E-Safety Policy

Introduction

E-safety encompasses Internet technologies and electronic communications such as mobile phones 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 experience.

The school's e-safety policy operates in conjunction with other policies including:

- Behaviour
- Anti-Bullying
- Data Protection
- Health and safety

It is also a key element of the school's PREVENT Duty and trained staff have considered this policy and its links to anti-radicalisation of all types.

E-safety depends on effective practice at a number of levels:

- Responsible ICT use by staff and students; 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.
- Safe and secure broadband, including the effective management of filtering systems.

School E-safety Policy

- The school's E-safety Leader is the I.T. Manager who will work in close liaison with the DSL (Designated Safeguarding Lead) and the Computing Leader.
- Our E-safety Policy has been agreed by the staff and approved by governors.
- The E-safety Policy will be reviewed annually.

Why is Internet Use Important?

The purpose of Internet use in school is:

- to raise educational standards
- to promote pupil achievement
- to support the professional work of staff
- to enhance the school's management information and administration systems.

Internet use is part of the statutory curriculum and a necessary tool for learning. It is an essential element in 21st century life for education, business and social interaction. Access to the Internet is therefore an entitlement for pupils who show a responsible and mature approach to its use. Our school has a duty to provide pupils with quality Internet access

Pupils will use the Internet outside school and will need to learn how to evaluate Internet information and to take care of their own safety and security.

How does Internet Use Benefit 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;
- access to experts in many fields for pupils and staff;
- professional development for staff through access to national developments, educational materials and effective curriculum practice;
- collaboration across support services and professional associations;
- improved access to technical support including remote management of
- networks and automatic system updates;
- exchange of curriculum and administration data with the Local Authority and DFE; access to learning wherever and whenever convenient.

How can Internet Use Enhance Learning?

- The school Internet access will be designed expressly for pupil use and includes 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.
- Internet access will be planned to enrich and extend learning activities.

- Staff should guide pupils in on-line activities that will support learning with 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, retrieval and evaluation.
- Pupils will regularly learn about online safety across the computing curriculum, they will participate in externally led workshops on how to make best and safest use of modern technology.

Pupils will be taught how to evaluate Internet content

- If staff or pupils discover unsuitable sites, the URL (address), time, content must be reported to the Local Authority helpdesk via the Online safety coordinator or network manager.
- School will ensure that the use of Internet derived materials by pupils and staff complies with copyright law.
- Pupils should be taught to be critically aware of the materials they are shown and how to validate information before accepting its accuracy.

Managing Internet Access

- The school's information management systems are secured by Hampshire County Council.
- Locally, virus protection will be installed and updated regularly.
- The school uses broadband with appropriate firewall and filters as recommended by HCC.

Email

- Pupils may only use approved e-mail accounts on the school system.
- Pupils must immediately tell a teacher if they receive offensive e-mail.
- Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.
- Whole class or group e-mail addresses should be used in school
- Access in school to external personal e-mail accounts may be blocked.
- E-mail sent to external organisations should be written carefully in the same way as a letter written on school headed paper. The E-safety officer has access to all e-mail correspondence.
- The forwarding of chain letters is not permitted.

Published content and 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.
- The E-safety officer will have overall editorial responsibility and ensure that content is accurate and appropriate.

Publishing pupils' images and work

- Pupils' full names will not be used anywhere on the website, particularly in association with photographs.
- Written permission will be obtained from parents or carers before photographs of pupils are published on the website.

Social Networking

- Social networking sites and newsgroups will be blocked unless a specific use is approved.
- Pupils will be advised never to give out personal details of any kind which may identify them or their location. Examples would include; real name, address, mobile or landline numbers, school, names of friends, specific interests and clubs etc.
- Pupils and parents will be advised that the use of social network spaces outside school is likely to be inappropriate for primary aged pupils.

Filtering

- The school will work in partnership with the Service Provider to ensure filtering systems are as effective as possible.
- If staff or pupils discover unsuitable sites, the URL, time and date must be reported to the E-safety Leader.

Video Conferencing

- IP videoconferencing should use the educational broadband network to ensure quality of service and security rather than the Internet.
- Pupils should ask permission from the supervising teacher before making or answering a videoconference call.
- Videoconferencing will be appropriately supervised for the pupils' age.

Managing Emerging Technologies

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.
- Staff should not use mobile phones to take pictures or videos of children.
- Staff should only use digital cameras which have been provided by the school. Mobile phones are not permitted for use anywhere in school, around the children. This applies to members of staff and other visitors to the school. Mobile phones may only be used in office areas, staffroom etc. The only exception to this is staff taking a mobile phone with them on a school trip/visit outside of school, for use in emergencies only.
- Children who bring mobile phones to school are required to hand them in to the school office staff every morning and devices are collected at home time.

The Prevent Duty and Online safety

- All schools have a duty to ensure that children are safe from terrorist and extremist material when accessing the internet in schools. We have an important role to play in equipping children to stay safe on line. Internet safety is integral to our computing curriculum.
- Our staff are aware of the risks posed by online activity of extremists and have a duty to take action if they believe the well -being of any pupil is being compromised.

Protecting Personal Data

- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 2018.

Authorising Internet Access

- The school I.T. Manager will maintain a current record of all staff and pupils who are granted internet access.
- All staff must read and sign the 'Acceptable Use of IT Policy' before using any school IT resources.

Assessing Risks

- In common with other media such as magazines, books and video, some material via the internet is unsuitable for pupils. The school will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither the school nor Hampshire County Council can accept liability for the material accessed, or any consequences of Internet access.
- The governors and Headteacher will monitor compliance with the E-safety policy

Handling E-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 teacher.
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.
- Pupils and parents will be informed of the complaints procedure.
- Sanctions may include; informing parents/carers, withdrawal of internet or computer access for a period, notifying the Police.

Communication of Policy

Pupils

- Rules for Internet use will be posted in all classrooms.
- Pupils will be informed that Internet use will be monitored.
- Advice on e-safety will be introduced at an age appropriate level to raise the awareness and importance of safe and responsible internet use.

Staff

- All staff will be given the School E-safety Policy and its importance explained.
- All staff will be trained in Safeguarding procedures, including elements of e-safety and The Prevent Duty.
- Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.

Parents

- Parents' attention will be drawn to the School E-safety Policy in newsletters and on the school Web site.
- The school will also organise E- safety workshops to support parents' understanding of how to best safeguard their children against potential online dangers.

Updated January 2021

Appendix A: Letter to Parents

Dear Parents,

At Ashley Junior School we aim to provide a high quality learning environment for your child, using the best resources and equipment available. As part of this aim, we encourage children to make use of the Internet for research work and to extend their learning activities. The Internet allows us to access a wealth of exciting, informative and up-to-the-minute information.

In order to combat the problem of children accessing unsuitable material through the Internet, we use an Internet Service Provider which has been recommended by Hampshire County Council. This Internet Service Provider filters out the material which is unsuitable for children and stops them from being able to view it on the school computers.

We also operate strict rules for using the Internet (see below) and the children are only allowed to access the Internet when being supervised by a member of staff. We also make sure that all the computer screens can be clearly seen by the member of staff at all times and that the children are guided in their searches to ensure that they make safe and profitable use of the Internet.

The Internet is an exciting and stimulating resource which will enhance your child's education. It will also assist us in ensuring that your child develops a good understanding of Information Communication Technology which is so important in today's world.

RULES FOR RESPONSIBLE INTERNET USE

- We always treat the computer equipment with care and respect.
- We only use the Internet when a teacher has given us permission and they are supervising us.
- We write a Search Plan if we need to look at a lot of web sites.
- We always write on our work where we have got any Internet information from.
- We tell a teacher straight away if we find something unpleasant.
- We never try to find unpleasant material on purpose.
- Our files will be checked by our teachers to make sure we are keeping to the rules
- We only send polite e-mail messages to the people we know at the addresses our teacher gives us.
- We ask a teacher to check our e-mail messages before we send them.
- We do not give our address or 'phone number, or arrange to meet anyone, over the Internet.

If we don't keep to the rules:

- We might have to stop using the Internet.
- Our parents might have to be told.

Yours sincerely,

Appendix B:

Staff Information Systems Code of Conduct

- To ensure that staff are fully aware of their professional responsibilities when using information systems, they are asked to sign this code of conduct. Staff should consult the school's e-safety policy for further information and clarification.
- The information systems are school property and I understand that it is a criminal offence to use a computer for a purpose not permitted by its owner.
- I will ensure that my information systems use will always be compatible with my professional role.
- I understand that school information systems may not be used for private purposes, without specific permission from the headteacher.
- I understand that the school may monitor my information systems and Internet use to ensure policy compliance.
- I will respect system security and I will not disclose any password or security information to anyone other than an appropriate system manager.
- I will not install any software or hardware without permission.
- I will ensure that personal data is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely.
- I will respect copyright and intellectual property rights.
- I will report any incidents of concern regarding children's safety to the school e-safety Leader or the Designated Safeguarding Lead
- I will ensure that any electronic communications with pupils, parents and colleagues are compatible with my professional role.
- I will promote e-safety with pupils in my care and will help them to develop a responsible attitude to system use and to the content they access or create.

The school may exercise its right to monitor the use of the school's information systems, including Internet access, the interception of e-mail and the deletion of inappropriate materials where it believes unauthorised use of the school's information 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.

I have read, understood and agree with the Information Systems Code of Conduct.

Signed: **Print Name:**

Date:

Appendix C:

These rules help us to stay safe on the Internet

- **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 webpage we are not sure about.**
- **We only email people an adult has approved.**
- **We send emails that are polite and friendly.**
- **We never give out personal information or passwords.**
- **We never arrange to meet anyone we don't know.**
- **We do not open e-mails sent by anyone we don't know.**
- **We do not use internet chat rooms.**