SHERBORNE HOUSE SCHOOL

E-Safety Policy

This policy applies to all pupils in the school, including EYFS

Created	**July 2015**
Revised	**November 2016**
Date for revision	**July 2018**

E-SAFETY POLICY (including Cyber Bullying)

Sherborne House School and EYFS

Sherborne House 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 need to plan to integrate the 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. It is built on the following five core principles:

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 e-safety 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 Headteacher is responsible for ensuring, so far 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 System 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.

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.

1) 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.

2) 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.

3) 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.

4) 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:

- All pupils will cover e-safety as part of the PSHE curriculum and will engage in discussion when computers are used in lessons and in assemblies.
- Every classroom and the computer suite has e-safety guideline posters displayed.
- A parent workshop on e-safety is held to explain school policy and procedures whereby parents are strongly encouraged to discuss e-safety at home with their children.
- Parents must discuss with their children and sign the 'Responsible Internet Use Letter' sent home in the Autumn term.

5) Pupils' Evaluation of Internet content

Inappropriate material should not be visible to pupils using the Web is not easy to achieve and cannot be guaranteed. Staff must therefore source prior to the lesson appropriate websites when engaging in research. The ICT systems manager will collate these and add to the Intranet page. 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. The teacher must immediately report this site ICT Systems 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.
- research techniques including the use of subject catalogues and search engines.
- to question the validity, currency and origins of information – key information handling skills.
- use alternative sources of information for comparison purposes.
- to understand that 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.

Pupils will also be taught that:

- If anyone discovers unsuitable sites, the URL (address) and content must be reported to the Internet Service Provider via the ICT Systems Manager.
- 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.

6) 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.

7) 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.

8) Cyber Bullying (to be read in conjunction with the Anti-Bullying and PSHE Policy)

- Cyber bullying is defined as the use of digital technologies with the intent to offend, humiliate, threaten, harass or abuse somebody
- Cyber bullying includes, for example, nasty messages, comments or posts via text, email or online. Embarrassing photos, fake profiles and rumours or lies can also take the form of bullying.
- Pupils are taught the following strategies to prevents cyber bullying:
  - Never respond and never delete
  - Take a screenshot as a record
  - Block and report
  - Talk to someone about it
  - Assess how serious it is
  - Protect your privacy - only be friends with people you know
  - Report any abuse to an adult
- Regular discussion and visits from external speakers ensure that countering cyber-bullying remains high profile among, staff, pupils and parents

9) 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 by the ICT Systems Manager before pupils are allowed to use a new technology in school.

10) 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.

11) 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.

12) 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 3 of this policy.

13) 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 'over blocking'.
- As part of the above the school should consider carefully how to manage the access to 3G and 4G in school or on trips (where applicable)

14) 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.

15) Staff consultation and training

- The school will ensure that all staff have undertaken appropriate e-safety training currently through Edu care training. **Child Exploitation & Online Safety for Education**
- 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 e-safety.

16) Technical provision, filters, safeguards and monitoring

- The school uses a Sophos Unified Threat Management (UTM) 9 device to protect and filter our school's network and internet filtering. All devices connected to the wired or wireless network are protected and filtered at levels suitable for our school environment.

- On top of the UTM we also use Impero Server* to monitor what is typed by all users, which searches for keywords such as drugs, cyber bullying, pornography, self-harm, radicalisation etc. The latest installed version helps ensure that we comply with the Keeping Children Safe in Education Act statutory guidance that came into effect September 2016.

- Our printing is also monitored via Papercut*, and records images of all print jobs, so we can monitor any inappropriate images or text being printed.

- *Impero and Papercut are not available on iPads.

17) Maintenance of ICT system security

- The school ICT systems will be reviewed regularly (termly) with regard to security in conjunction with the ICT Systems Manager.
- Virus protection will be installed and updated regularly by ICT Systems Manager.
- Memory sticks and other such portable storage devices may not be brought into school without specific permission from ICT Systems Manager and will require virus scanning before use.
- Unapproved system utilities and executable files will not be allowed in pupils' work areas or attached to e-mail.