# Online Safety and Acceptable Use Policy

**Purpose**

The purpose of Halifax Primary’s safeguarding policy is to provide a secure framework for the school in safeguarding and promoting the welfare of those pupils who attend our school.

**Audience**

- School Governors
- Staff
- Pupils & Parents

**Related Policies**

- Safeguarding Policy
- Acceptable use of ICT
- Social Networking

**Policy Re - approved**

September 2016

**Policy updated to reflect new guidance**

January 2018 – updated to reflect changes in terminology

**Future Policy Review**

September 2020
Core Principles of Online Safety

The internet is as commonplace as the telephone or the television and its effective use is an essential life skill. Unmediated internet access brings with it the possibility of placing pupils in embarrassing, inappropriate and even dangerous situations. Schools need a policy to help to ensure responsible use of the internet and the safety of pupils.

A recommended Online Safety Policy is built on the following three core principles:

Educating young people to be responsible users of ICT

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 must also learn how to recognise and avoid these risks for themselves as they grow older – to become “internet wise”. The precise nature of the risks faced by young people will change over time as new technologies, fads and fashions take hold, but there are general principles of safe online behaviour that apply to all situations, for example; pupils need to know how to react if they come across inappropriate material and how to protect their personal information on the internet. They should also be able to evaluate critically the quality of the material they find on the internet. The balance between educating pupils to take a responsible approach and the use of regulation and technical solutions must be judged carefully.

Guided educational use

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

Regulation and control

Online safety depends on staff, schools, governors, advisers, parents and, where appropriate, the pupils themselves taking responsibility for the use of internet and other communication technologies such as mobile phones. The use of a finite and expensive resource, which brings with it the possibility of misuse, requires regulation. In some cases, access within schools must simply be denied, for instance unmoderated chat rooms present immediate dangers and are usually banned. Fair rules, clarified by discussion and prominently displayed at the point of access will help pupils make responsible decisions.

This document describes strategies that help to ensure responsible and safe use of online technology. They are based on developing responsibility, guiding pupils towards educational activities and limiting access. There are no straightforward or totally effective solutions and staff, parents and the pupils themselves must remain vigilant.
Halifax Primary School Online Safety Policy

1 Who will write and review the policy?

- Our Online Safety policy has been written by the school, building on the Suffolk County policy and government guidance. It has been agreed by the senior management and approved by governors following discussions with the Parents and School Council. It will be reviewed annually.

2 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 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.
- Internet access is an entitlement for students who show a responsible and mature approach to its use.
- 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.

3 How does the internet benefit education?

Benefits of using the internet in education include:

- Access to world-wide educational resources including museums and art galleries;
- Inclusion in government initiatives
- 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;
- Exchange of curriculum and administration data with the LA and DfE.

4 How will internet use enhance 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.
• 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 should 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, evaluation and retrieval. They will sign the parent and pupil Acceptable Use Policy.

5 How will pupils learn to evaluate internet content?

• 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.
• Schools should ensure that the use of internet derived materials by staff and by 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. Pupils in EYFS and Key Stage 1 will need close supervision.
• Pupils will be taught to acknowledge the source of information used and to respect copyright when using internet material in their own work. Pupils in EYFS and Key Stage 1 will need close supervision.

6 How will email be managed ensuring safety for pupils?

• Pupils may only use approved email accounts on the school system.
• Pupils must immediately tell a teacher if they receive offensive email.
• Pupils must not reveal details of themselves or others in email communication or via a personal web space, such as address or telephone number, or arrange to meet anyone.
• Personal email or messaging between staff and pupils should not take place.
• Whole-class or group email addresses should be used at Key Stage 1 and below, rather than individual messaging.
• Email sent to an external organisation should be written carefully and authorised before sending, in the same way as a letter written on school headed paper.

7 How should website/learning platform content be managed?

• The point of contact on the website should be the school address, school email 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 clearly identified.
• Pupils’ full names will only be used to identify learning platform accounts, and will not be published in association with photographs.
• Written permission from parents or carers will be obtained before photographs of pupils are published on the school website.
• The Headteacher or Computing Lead will take overall editorial responsibility and ensure that content is accurate and appropriate.
• The website should comply with the school's guidelines for publications.
• The copyright of all material must be held by the school, or be attributed to the owner where permission to reproduce it has been obtained.

8 Newsgroups, Email Lists and Forums

• Newsgroups will not be made available to pupils unless an educational requirement for their use has been demonstrated.
• Access to forums that are moderated by a responsible person or organisation and are directly linked to an educational activity will be permitted.

9 Chat and instant messaging

• Pupils will not be allowed access to public or unregulated chat rooms.
• Pupils will not access social networking sites for example ‘My Space’, ‘Facebook’ or ‘Bebo’.
• Children should use only regulated educational chat environments. This use will be supervised and the importance of chat room safety emphasised.
• Any form of bullying or harassment is strictly forbidden.
• A risk assessment will be carried out before pupils are allowed to use a new technology in school.
• No member of staff should engage in direct communication (in or out of school) of a personal nature with a pupil who is not a member of their direct family, by any means, for example, but not limited to, SMS text message, email, instant messaging or by telephone.

10 Personal websites and blogs

• Pupils will not access social networking sites for example ‘My Space’ or ‘Bebo’.
• When publishing material to websites and elsewhere, pupils should consider the thoughts and feelings of those who might view the material. Material that victimises or bullies someone else, or is otherwise offensive, is unacceptable.

11 Photographic, video and audio technology

• It is not appropriate to use photographic or video devices in toilets or in classrooms should pupils be inappropriately dressed.
• Care should be taken when capturing photographs or video to ensure that all pupils are appropriately dressed.
• Staff may use photographic or video devices (including digital cameras and mobile phones) to support school trips and curriculum activities. These must be school devices.
• Audio or video files may only be downloaded if they relate directly to the current educational task being undertaken. These files must be downloaded to the school server, not cloud based storage, and deleted once they have no further use.
• Pupils should always seek the permission of their teacher before making audio or video recordings within school.

12 How can emerging technologies be managed?

• Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.
• Personal use mobile phones will not be used during lessons or formal school time by staff, volunteers or pupils. Pupils, who bring personal devices to school, must hand these in to the office at the beginning of the school day and collect them on their way home.
• The use of blog messaging on social network sites is strictly forbidden.

13 How will internet access be authorised?

• The school will keep a record of all staff and pupils who are granted internet access. The record will be kept up-to-date, for instance a member of staff may leave or a pupil’s access be withdrawn.
• At Key Stage 1, access to the internet will be by adult demonstration with occasional directly supervised access to specific, approved on-line materials.
• 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. Please see the pupil/parent Acceptable Use Policy in this document.

14 How will the risks be assessed?

• 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. Neither the school nor the Multi-Academy Trust can accept liability for the material accessed, or any consequences of internet access.
• The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990.
• Methods to identify, assess and minimise risks will be reviewed regularly.
• The Headteacher will ensure that the Online Safety policy is implemented and compliance with the policy monitored.
• Access is strictly forbidden to any websites that involve gambling, financial scams or pornographic material.

15 How will filtering be managed?

• The school will work in partnership with parents; the LA, DfE and the Internet Service Provider to ensure systems to protect pupils are reviewed and improved.
• If staff or pupils discover unsuitable sites, the URL (address) and content must be reported to the Internet Service Provider via the Computing Lead.
• Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.
• Any material that the school believes is illegal must be referred to the Internet Watch Foundation (www.iwf.org.uk).
• Filtering strategies will be selected by the school, in discussion with the filtering provider where appropriate. The filtering strategy will be selected to suit the age and curriculum requirements of the pupil.

16 How will the policy be introduced to pupils?

• Rules for internet access will be posted in all rooms where computers are used.
• Pupils will be informed that internet use will be monitored.
• Instruction in responsible and safe use should precede internet access.
• Online Safety lessons will be included in the PSHE (physical, social, health, emotional) programme covering both school and home use.

17 How will staff be consulted and made aware of this policy?

• All staff must accept the terms of the ‘Responsible Internet Use’ statement before using any internet resource in school.
• All new staff will be taken through the key parts of this policy as part of their induction.
• All new staff will be provided with a copy of this policy, which they will be expected to sign and return for school records.
• All staff including teachers, supply staff, classroom assistants and support staff, will be provided with the school’s Online Safety Policy and have its importance explained. Staff should be aware that internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.
• The monitoring of internet use is a sensitive matter. Staff who operate monitoring procedures will be supervised by senior management.
• Staff development in safe and responsible internet use and on the school internet policy will be provided as required.
• Breaching this Online Safety Policy may result in disciplinary action being taken and access to ICT being restricted or removed.

18 How will ICT system security be maintained?

• The school ICT systems will be reviewed regularly with regard to security.
• Virus protection will be installed and updated regularly.
• Security strategies will be discussed with the LA, particularly where a wide area network connection is being planned.
• Personal data sent over the internet will be encrypted or otherwise secured.
• Unapproved system utilities and executable files will not be allowed in pupils’ work areas or attached to email.
• Files held on the school’s network will be regularly checked and must be deleted when of no further use.

19 How will complaints regarding internet use be handled?

• Responsibility for handling incidents will be delegated to the Online Safety Lead
• Any complaint about staff misuse must be referred to the Headteacher.
• Pupils and parents will be informed of the complaints procedure.
• Parents and pupils will need to work in partnership with staff to resolve issues.
• Sanctions available include:
  - interview/counselling by class teacher/ Headteacher;
  - informing parents or carers;
  - removal of internet or computer access for a period
• There may be occasions when the police must be contacted. Early contact could be made to establish the legal position and discuss strategies. Advice sought should include how best to preserve any possible evidence.

20 How will parents’ support be enlisted?

• Parents’ attention will be drawn to the school’s Online Safety Policy in newsletters, the school brochure and on the school website.
• Internet issues will be handled sensitively to inform parents without undue alarm.
• A partnership approach with parents will be encouraged. This could include practical sessions and suggestions for safe internet use at home.
• Advice on filtering systems and educational and leisure activities that include responsible use of the internet will be made available to parents.
• Interested parents will be referred to organisations such as PIN (Parents Information Network), Parents Online and NCH Action for Children (see websites in appendices)

21 How is internet used across the community?

• Adult users will need to sign the acceptable use policy.
• Parents/carers of children will be required to sign an acceptable use policy on behalf of the child.

22 Staff Personal Use and Privacy

In the course of normal operations, ICT resources are to be used for business purposes only. The school permits limited personal use of ICT facilities by authorised users subject to the following limitations:

• Personal use must be in the user’s own time and must not impact upon work efficiency or costs.
• The level of use must be reasonable and not detrimental to the main purpose for which the facilities are provided.
• Personal use must not be of a commercial or profit-making nature.
• Personal use must not be of a nature that competes with the business of the school or conflicts with an employee’s obligations e.g. eBay selling account.

Personal use of the Internet must not involve attempting to access the categories of content described above that is normally automatically blocked by web filtering software.
Halifax Primary School Staff Code for Acceptable Use

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 Online Safety and Acceptable Use 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 use of my laptop in school or use of the school network will 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 (on an encrypted memory stick, for instance) 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’s Online Safety Lead or the Designated Safeguarding Lead.
- I will ensure that any electronic communications with pupils are compatible with my professional role.
- I will promote online safety with students 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 email 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.
Halifax Primary School Pupil Code for Acceptable Use

The school has installed computers and Internet access to help our learning. These rules will keep everyone safe and help us to be fair to others.

- I will ask permission from an adult in school before using school technology or accessing the internet.
- I will only use school technology to support my learning and under the direction of an adult.
- I understand that the school may check my computer files and may monitor the Internet sites I visit.
- I will not share my usernames and passwords or any personal information with anyone other than a trusted adult.
- I will not install any software or hardware without permission.
- I will not copy other people’s work and say that it is mine.
- If I have any worries or concerns about images or content I see online I will report this to the school’s Online Safety Lead, Mr Doyle or the Designated Safeguarding Lead, Mrs Landers.
- I will ensure that all communications with other people are responsible and respectful.
- I understand that these rules are designed to keep me safe and that if they are not followed, consequences will be applied and my parent/carer may be contacted.