Harrington Hill Primary School

E-Safety and Acceptable use of ICT Policy

REVIEWED: December 2018

NEXT REVIEW DATE: December 2019

Adopted:

Striving for Excellence. Achieving Together.

Striving for excellence. Inspiring to achieve collaboratively through respect, happiness and creativity. We are independent and reflective for continuous improvement.

Our Statement:

Our e-safety policy has been written by the Pastoral Lead and Computing Lead. It has been agreed by the senior leadership and approved by governors following discussions with the School Council. It will be reviewed annually.

Rationale

This document is a statement of the schools commitment to ensuring Safe Use of the internet.

Harrington Hill takes the safety of all children and adults very seriously. This policy is written to protect all children and adults. Harrington Hill believes in the educational benefits of ICT use and seeks to educate young people to become effective, reflective and responsible users. We recognise that e-Safety encompasses not only internet technologies, but also electronic communications such as mobile phones and wireless technology.

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.

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.

Aims

Harrington Hill aims to make the school community aware of the risks associated with electronic communication and to take all reasonable measures to ensure that those risks are controlled, minimised and where possible removed. E-Safety is the responsibility of the **whole community.**

Internet technologies and electronic communications provide children and young people with opportunities to broaden their learning experiences and develop creativity in and out of school. However, it is also important to consider the risks associated with the way these technologies can be used.

This E-Safety Policy should recognise and seek to develop the skills that children and young people need when communicating and using these technologies properly, while keeping safe and secure, and acting with respect for others.

We aim to ensure all members of the school community – children, teachers, parents and governors – are aware of the need for safe and responsible internet use; the issues surrounding internet safety are discussed and that internet use supports schools' educational aims.

RISKS

Risks to e-safety are caused by people acting inappropriately or even illegally. In school teachers and support staff are the first line of defence; their observation of behaviour is essential in detecting danger to pupils and in developing trust so that issues are reported.

- Receiving inappropriate content;
- Predation and grooming;
- Requests for personal information;
- Viewing 'incitement' sites;
- Bullying and threats;
- Identity theft;
- Publishing inappropriate content;
- Online gambling;
- Misuse of computer systems;
- Publishing personal information;
- Hacking and security breaches;
- Corruption or misuse of data;
- Cyberbulling (see antibullying policy)

How does the internet benefit education?

Harrington Hill believes that developing effective practice in internet use for teaching and learning is essential. 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 functions.

Pupils use the Internet widely outside school and will need to learn how to evaluate internet information and to take care of their own safety and security. The school internet access will be designed expressly for pupil use and will include filtering appropriate to the age of pupils.

How will internet use enhance learning?

Pupils will be taught what internet use is acceptable and what is not and given clear objectives for internet use. The key components of this teaching will be:

- 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, retrieval and evaluation.

How will children be taught to assess Internet content responsibly?

Pupils may occasionally be confronted with inappropriate material, despite all attempts at filtering. Pupils should 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 incident immediately to the teacher. The school will ensure that the copying and subsequent use of internet derived materials by staff and pupils complies with copyright law.

- Children will be taught ways to validate information before accepting it is necessarily accurate.
- Children will be taught to acknowledge the source of information, when using internet material for their own use.
- Children will be made aware that the writer of an e-mail, or the author of a web page might not be the person claimed.
- Children will be encouraged to tell a teacher immediately if they encounter any material that makes them feel uncomfortable.
- Children will be taught how to use a search engine responsibly and effectively.

How will e-mail be managed ensuring safety for pupils?

The government encourages the use of e-mail as an essential means of communication for both staff and pupils. Directed e-mail use can bring significant educational benefits and interesting projects between neighbouring villages and between continents have been created, often with the help of “project finder” sites.

- 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 details of themselves or others in e-mail communication or via a personal web space, such as address or telephone number, or arrange to meet anyone.
- The forwarding of e-mails is not permitted.
- Messages sent using the school domain should be regarded in the same way as messages written on school headed paper.

Social Media

- Any form of bullying or harassment is strictly forbidden.
- The school will block/filter access to social networking sites;
- Newsgroups will be blocked unless a specific use is approved;
- Children will be taught about the role of CEOP (Child Exploitation and Online Protection) and how to contact such organisations;
- Pupils will be advised never to give out personal details of any kind which may identify them and / or their location. Examples would include real name,

address, mobile or landline phone numbers, school attended, IM and e-mail addresses, full names of friends, specific interests and clubs etc.;

- Pupils should be advised not to place personal photos on any social network space;
- They should consider how public the information is and consider using private areas;
- Advice should be given regarding background detail in a photograph which could identify the student or his/her location eg. house number, street name or school;
- Teachers should be advised not to run social network spaces for student use on a personal basis.
- Older pupils will be taught about the dangers of sexting, grooming and sharing inappropriate photos online. They will be made aware of dangers posed by different kinds of social media, and the kinds of dilemnas or problems they could face as a teenager whilst using it. Discussion of pornography, adult social media apps and consent will be a feature of sex and relationships education in higher KS2. Sexting describes the use of technology to generate images or videos made by children under the age of 18 of other children; images that are of a sexual nature and are indecent. The content can vary, from text messages to images of partial nudity to sexual images or video. These images are then shared between young people and/or adults and with people they may not even know. Young people are not always aware that their actions are illegal and the increasing use of smart phones has made the practice much more common place.

How will publishing on the Web be managed?

Many schools have created websites that inspire children to publish work to a high standard, for a very wide audience. A website can celebrate children's work, promote the school and publish resources for projects or homework. Ground rules are important to ensure that the website reflects the school's ethos and that information is accurate and well presented.

As Harrington Hill School website can be accessed by anyone on the internet, the security of staff and children is paramount. Although common in newspaper reports, the publishing of children's names beside photographs that identify individuals will not occur.

Editorial responsibility will lie with the Head Teacher even where help has been established to maintain the site. This is in order to ensure that content is accurate and quality of presentation is monitored.

Staff and children will be made aware that the quality of their work published on the web needs to reflect the standard of work expected at Harrington Hill School.

- All material must be the author's own work, or where permission to reproduce has been obtained, clearly marked with the copyright owner's name.
- The point of contact on the website should be the school address and telephone number. Home information or individual email identities will not be published.
- Staff will notify the school if they do not want film footage of themselves on the website.

Use of Images

- Images that include pupils will be selected carefully and will not enable individual pupils to be clearly identified unless there is parental permission;
- Pupils' full names will not be used anywhere on the website, particularly in association with photographs;
- Written permission from parents or carers will be obtained before images of pupils are electronically published.

Photographic, video and audio technology

- 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 iPads) to support school trips and curriculum activities.

How will internet access be authorised?

The school should allocate internet access for staff and pupils on the basis of educational need. It should be clear who has internet access and who has not. In a primary school, where pupil usage is fully supervised, government guidance is that all pupils in a class might be authorised as a group. As most pupils will be granted internet access, it may be easier to manage lists of those who are denied access.

- At Key Stage 1, access to the internet will be by adult demonstration with occasional directly supervised access to specific, approved on-line materials.
- At Key Stage 2, when it is part of a scheme of work, then internet access will be granted to a whole class, after a suitable education in responsible internet use.

How will the risks be assessed?

It is difficult to remove completely the risk that children might access unsuitable materials via the school system whatever safeguards are put in place.

- Due to the international scale and linked nature of information available via the internet, it is not possible to guarantee that unsuitable material will never appear on a terminal.

- Neither the school nor the Local Authority can accept liability for the material accessed, or any consequences thereof.
- The use of computer systems without permission or for purposes not agreed by the school could constitute a criminal offence under the Computer Misuse Act 1990.
- Methods to identify, assess and minimise risks will be reviewed at the same time as the policy is reviewed.
- Staff, parents, governors and advisers will work to establish agreement that every reasonable measure is being taken.
- The Curriculum Leader for ICT and the headteacher will ensure that the policy is implemented effectively.

How will the school ensure Internet access is safe?

- The system the school will use is a blocking system operated by the London Grid for Learning.
- Children will be informed that internet use will be supervised and monitored
- The school will work in partnership with parents; the Local Authority, DfE and the Internet Service Provider to ensure systems to protect children are reviews and improved.
- Teachers will ensure that occasional checks are made to ensure that the filtering methods selected are effective in practice.
- In the unlikely event that staff or children discover unsuitable sites, the URL (address) and content will be reported to the Internet Service Provider via the Curriculum Leader for ICT and blocked through the schools computer filters.

How will the security of school ICT systems be maintained?

- Security strategies will be discussed with the Local Authority.
- The security of the whole system will be reviewed with regard to threats to security from internet access.
- Personal data sent over the internet will be encrypted or otherwise secured.
- Virus protection will be installed and updated regularly.

How will incidents regarding internet safety and inappropriate use be handled?

Parents, teachers and students must know how and where to report incidents. All incidents will be reported and logged by the online safety officer, and if necessary, the safeguarding lead for the school.

Prompt action may be required when an incident is reported. The facts of the case will need to be established, for instance whether the internet use was within or outside school.

In the case of a minor, internal transgression of the rules it may be dealt with by the teacher as part of normal class discipline. Other situations could potentially be more serious and a range of sanctions and/or safeguarding actions will be required, linked to the school's behaviour and/or safeguarding policy.

• Responsibility for handling incidents will be delegated to either the online safer officer or a senior member of staff. In high risk incidents, Police, social workers and other relevant key workers may be involved.

Any incident that is logged by the school, whether internal or external, may be used in confidentiality by the online safety working group at Harrington Hill in order to identify key actions required to resolve the incident and/or use the incident as evidence supporting a change or amendment to the schools online safety policies and procedures.

Where incidents are external to the school and cannot be dealt with using the schools own processes they will be referred to another relevant body within our key and local contacts, in line with the 'referring safeguarding concerns' policy in line with Child Protection procedure and/or the schools PREVENT statement 2016.

• Any complaint about staff misuse must be referred to the Head Teacher.
• Pupils and parents will be informed of the complaints and incidents procedure.
• Parents and pupils will need to work in partnership with staff to resolve issues, in particular by contributing to and representing themselves at the school's Online safety group meetings.

How will staff and children be consulted?

- Rules for Safe Use of Internet access will be discussed with children through school (in class and assemblies) and school council and posted near computer systems.
- All staff including teachers, supply staff, classroom assistants and support staff and parents will be made aware these rules, and their importance explained.
- Parents' attention will be drawn to the policy in newsletters and on the school website.

How will parent's support be enlisted?

The school believes it has a duty to help parents plan appropriate use of the Internet at home, and as such:-
• A careful balance between informing and alarming parents will be maintained.

- Joint home/school guidelines on issues such as safe internet use will be established.

Parents will be consulted regularly on online safety issues and concerns or suggestions arising from this will inform the creation and review of all online safety policies, procedures and teaching.

Safe Internet Use

These rules help us to be fair to others and keep everyone safe.

- I will ask permission before using the Internet.
- I will use only my own network login and password, which is secret.
- I will only look at or delete my own files.
- I understand that I must not bring software or disks/USB pens into school without permission.
- I will only email people I know, or my teacher has approved.
- The messages I send will be polite and sensible.
- I understand that I must never give my home address or phone number, or arrange to meet someone.
- I will ask for permission before opening an email or an email attachment sent by someone I do not know.
- I will not use Internet chat.
- If I see anything I am unhappy with, or I receive messages I do not like, I will tell a teacher immediately.
- I understand that the school may check my computer files and the internet sites I visit.
- I understand that is I deliberately break the rules, I may not be allowed to use the internet or computers.

The school may exercise its right to monitor the use of the school's computer systems, including access to websites, the interception of email and the deletion of inappropriate materials where it believes unauthorised use of the school's computer system is or may be taking place, or the system is or may be taking place, or the system is or may be used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.

Think then Click

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.

We can send and open emails together.

We can write polite and friendly emails to people that we know.

E-Safety Incident Log

Child (ren)'s Full Name(s):_____

Date(s) of Birth: _____

Name of Contact Parent/Carer: _____

Contact Address: _____

_____

Brief Description of Incident
Action Taken

Signatures

Staff Member **Head Teacher**

_____ **_____**

Date of Incident: _____