Hiltingbury Junior School

IT, Internet and E-Safety Policy

Reviewed: **March 2016**

Hiltingbury School recognises the importance of School Technology to the whole school community and sees the World Wide Web and related technologies as being valuable resources. School Technology is defined as all school digital equipment and all school virtual spaces based within and outside the physical building.

Internet
Internet safety depends on staff, school governors, parents and, where appropriate, pupils themselves taking responsibility for the use of the Internet and associated communication technologies.

We recognise that, under certain circumstances, the Internet can give pupils access to undesirable information and images. We do all that we can to ensure pupils are protected from such information through the use of security software, limiting of features and by providing as safe as an environment as possible. The pupils are taught to use the facility sensibly and with proper consideration for others.

The following rules ensure the privacy and safety of members of our school community when using the Internet:

- Pupils are only referred to by their first names on our web pages
- Any images of pupils will not be labelled with their full names without prior permission of parent.
- Records of permission levels for use of pupil images are regularly updated for all staff to access.
- Pupils and staff will not reveal their personal details, and home addresses & telephone numbers on the web or in dialogue with other Internet users.
- A random selection of pupil E-mail will be regularly monitored each week.
- E-mail is restricted to the schools domain, so children cannot email outside of this at present.
- Pupils will not engage in dialogue or conversation with other Internet users without permission by a teacher. Online conversations within Google Classroom are recorded, as is use of comment functions in shared documents.
- Search Engines used by the pupils offer a filtered list of links and children are taught how to use these.
- Any pupil finding themselves uncomfortable or upset by anything they discover on the Internet should report it to a teacher immediately.
- Downloading of files is restricted to staff or pupils under supervision.
- Use of Google Apps in Education, including Mail, Classroom, Sites and Drive is monitored by teachers and IT Technician
- Hampshire restricts use of social media in school.
- All Internet access is filtered through a proxy server (HCC) to screen undesirable sites at source.
- Guidance on acceptable use of School Technology is included in the Staff Handbook

Contravention of the above rules will result in the withdrawal of Internet access privileges in the first instance. Records of contraventions are kept and monitored by Computing Subject leader and IT Technician in liaison with Deputy Headteacher.

E-Safety
Hiltingbury seeks to include e-safety within the wider sphere of citizenship believing that encouraging good digital citizenship is the key to pupils choosing safe practise at school and at home.

Pupils

When pupils join the school, parents are asked for their written consent for children to use Google Apps for Education. Without this consent children are not allowed to use the Google Apps suite of online resources. In addition the following rules are shared and reinforced regularly in Computing and PDL sessions:

1. I will not give out personal information such as my address, telephone number, parents' work address/telephone number, or the name and location of my school without my parents' or teacher's permission.
2. I will tell my parents or teacher right away if I come across any information that makes me feel uncomfortable.
3. I will never agree to get together with someone I "meet" online without first checking with my parents. If my parents agree to the meeting, I will be sure that it is in a public place and bring my mother, father or guardian along.
4. I will never send a person my picture or anything else without first checking with my parents or teacher.
5. I will not respond to any messages that are mean or in any way make me feel uncomfortable. It is not my fault if I get a message like that. If I do I will tell my parents or teacher right away so that they can take action on my behalf.
6. At home I will talk with my parents so that we can set up rules for going online.
7. I will not give out any passwords to anyone (even my best friends) other than my parents
8. I will be a good online citizen and not do anything that hurts other people or is against the law.

As pupils progress through the school, digital citizenship continues to be taught and monitored through the Computing and PDL schemes of work. The rules are exemplified and put into real situations allowing children to explore what they would do in simulated "real" situations. Children in every year group are invited to become 'Digital Leaders' to promote safe and responsible use of technology. The group meets weekly and are encouraged to share their views in forming the concept of digital citizenship. Our aim is always to empower children with safety knowledge so that they can use the World Wide Web with confidence and safety.

Pupil access to the World Wide Web

Children should only be using computers, laptops and chromebooks under the supervision of an adult. World Wide Web access is filtered by Hampshire County Council who are the schools service providers. However no filtering system is 100% efficient so children are encouraged to turn off the monitor and report immediately any inappropriate material to a relevant adult. If they self-censor they are to be congratulated and rewarded. If another pupil reports that a pupil is accessing inappropriate material then school sanctions will apply to the pupil accessing the material. Children are not permitted to use SMART phones or other personal mobile devices which access the internet in school.

Sanctions

Pupils who break the schools code of conduct as to the use of the Web and e-mail will be dealt with according to the severity of the breach. However for most first offences the pupil would have e-mail and Web rights withdrawn for a period of two weeks and their parents would be contacted. Any further breaches could result in the withdrawal of logon rights and pupils would only be able to practise ICT through a much restricted pupil desktop at set times defined by the network manager.

Staff rights and responsibilities

All staff can use School Technology

The school network can be used at any time that staff are permitted to be on the premises. If staff can access school technology online at home they are permitted to do so at any time. Hiltingbury encourages staff to develop a healthy work life balance but does not presume to tell staff when and when not to access school technology. Staff may use School Technology for professional or private use. Private use is encouraged as it leads to greater professional skills.

All School Technology use is subject to the following provisions as per the Staff Handbook:

- ICT includes a wide range of systems, including mobile phones, PDAs, digital cameras, email, social networking and that ICT use may also include personal ICT devices when used for school business.
- Only access the computer system with the login and password you have been given
- Do not access other people's files - No other user should have his or her system or data compromised through deliberate acts by any member of staff.
- Do not bring in CDs, DVDs or memory sticks from outside school and try to use them on the school computers
- The sending and receiving of personal e-mails and surfing the web for personal reasons is not allowed during working/directed hours
- understand that it is a criminal offence to use a school ICT system for a purpose not permitted by its owner
- Do not use the school ICT system to access inappropriate content
- School information systems, Internet and email may be monitored and recorded
- Do not disclose any password or security information to anyone other than an authorised system manager.
- Ensure that personal data is stored securely and is used appropriately, whether in school, taken off the school premises or accessed remotely. It must NOT be kept on removable storage devices.
- Photos must not be taken using a digital device of any child without first having checked if permission has been given by the parent – records are kept in SIMs. This is to avoid accidental downloading and storage of digital images of children which could potentially find themselves on a website.
- Respect copyright and intellectual property rights.
- Report any incidents of concern regarding children's safety to the schools e-Safety Coordinator, the Designated Child Protection Liaison Officer or Head teacher.
- The school may exercise its right to monitor the use of the school's information systems and Internet access, to intercept e-mail and to delete inappropriate materials where it believes unauthorised use of the school's information system may be taking place.
- Users are responsible for all e-mails or other digital media sent and any contacts made that may result in e-mails or other digital media being received
- Staff have a limited right to professional materials created or stored on the school network. Data that is created for professional reasons shall remain the property of the school and the creator. However if

the school wishes to share this data outside of the school then the creator must give his or her written permission. If the creator wishes to share materials made then they have a perfect right to do so. If a person leaves then a copy of all work created for the school such as planning must be left for the school to use or adapt in perpetuity within the school but must not be shared outside the school without the creator's written permission.

Any breach of these provisions will be dealt with according the severity of the breach. If the breach is a breach of law, the police will be called in straight away and all evidence will be preserved even to the non-use of the relevant School Technology. If the breach is less severe school disciplinary action would result through established channels.

Shared Data
At Hiltingbury we encourage staff to share data, over the school network and via our various virtual learning environments including Google Apps for Education. With this in mind a file naming protocol has been shared with staff that will help everyone to work together in a smart and safe way.
The only exception to this might be year group areas which often need tidying up at regular intervals. The year leader is responsible for this and should let his or her team know when they are carrying this out. If files or folders are to be deleted then the relevant users who created them need to informed in advance (suggest a week) so they can (if they wish) move data to their own private area in advance of the clean up.

Staff personal devices
The school benefits from staff using personal devices at school. If staff use these devices to take photos or videos of pupils for blogging or other educational purposes then these images should be regularly deleted. Staff should never use these images on websites not covered by parental agreement.

Blogging Guidelines and Rules
In addition to Year Group websites, teachers at Hiltingbury can choose to use a blog with their class. If they do so the following rules will apply.

Blogging is

- A great way to share good work done by pupils in the class with their family and Friends.
- A great way to showcase and share what you are doing in class with parents and prospective parents.
- A great way for pupils to write about what they want to write about.
- A real encouragement to write outside of school.
- One of the best ways to explore e-safety in a real way

Blogging Rules

- Teachers should always be the gatekeeper for all blog posts and comments on a school blog. This means that every post or comment must be checked before being published on the Internet.
    - Teachers shouldn't mark blog posts online as these comments are seen by everyone. Teachers may wish to use online writing as one more strand building to a complete picture of a child's strengths, weaknesses and possible targets.
    - If a teacher chooses to comment it must always be positive and teachers should only allow comments from others that are positive.

- If someone attempts to comment or attempts to post an Internet link this must be followed by the teacher to make sure it is suitable.
- A blog post that contains a picture or video of a child should not contain their name. The pupil and those who know the pupil will recognise who they are without needing to be named.
- Pictures or videos on the class blog should only contain children whose parents have given their consent to this.
- Blog posts that don't contain a child's image should only refer to them by their first name, initials or a blogging pseudonym.
- Teachers should refrain from publishing any blog that contains ages, addresses or personal information that could be used to target a child outside school. If a child writes about his or her family they shouldn't use their first name and should publish it with their initials or pseudonym instead.

Social Networking

Staff to pupils or parents
Staff should not be accepting pupils[1] or parents as "friends"[2] on any social networking type site[3] where staff or their friends share private information[4].

1. Pupils refers to current pupils and ex pupils below the age of 18
2. Friends refers to any type of acceptance into private social sphere
3. Social networking can occur on Facebook, Bebo, Twitter type sites and on gaming networks such as PS3 or Xbox 360
4. This is to distinguish between social networks set up for education uses such as Studywiz, Moodle and Google Docs or others that can be used online and those used for private social reasons.

The reasoning behind this is as follows

- Staff may share behaviour that may be acceptable privately but is not appropriate for under 18's.
- Staff may find private pictures or information shared and used by pupils or their parents maliciously.
- The school believes that is good for staff to have personal spaces away from the demands of school and supports staff in saying no by officially stating this in policy.

Exceptions
Where parents are within the social sphere of Hiltingbury staff then it may be acceptable to accept parents as friends.

Staff should avoid commenting on pupils, parents or the school on any social network which is in anyway public. All staff online communication to pupils should be

- Clear and unambiguous leaving pupils clear as to meaning and direction
- Free of mixed meanings or rude undertones
- Communicated in such a way as it can be read and understood by their parents

Staff are advised in the Staff Handbook to avoid communicating disciplinary items to pupils using technology. Staff should to the best of their ability avoid communicating known contentious items to parents by online media.

FORMULATION OF POLICY: January 2016

Staff agreed the draft policy: January 2016

It was ratified by governors on: March 2016

REVIEW DATE: Autumn 2019