Hester's Way Primary School
Acceptable User Policy

Introduction

This policy outlines the acceptable use of ICT equipment at our school by staff, volunteers and pupils. It also includes use of access to the internet, use of emails and social media, use of mobile phones, photography and film permissions as well as data protection whilst using hardware. This policy is available on the school website and parents/carers can ask for a free copy from the school office.

Internet access in school

The purpose of internet access in schools is to raise educational standards, support the professional work of staff and enhance the school's management, information and business administration systems.

Teachers and pupils will have access to web sites worldwide offering educational resources, news and current events.

In addition, staff will have the opportunity to: access educational materials and good curriculum practice; communicate with the advisory and support services, professional associations and colleagues; exchange curriculum and administration data with the LA and DfES; receive up-to-date information and participate in government initiatives.

The computer network, Learn-pads, Ipads and laptops are owned by the school, and may be used by children to further their education and by staff to enhance their professional activities including teaching, research, administration and management. The school's AUP Policy has been drawn up to protect all parties - pupils, staff, volunteers and the school.

The school reserves the right to examine or delete any files that may be held on its computer system or to monitor any internet sites visited.

- All internet activity should be appropriate to staff professional activity or the children's education
- Access should only be made via the authorised account and password, which should not be made available to any other person
- Users are responsible for all E-mails sent and for contacts made that may result in E-mail being received; school emails should be used in a professional manner
- Use for personal financial gain, gambling, political purposes or advertising is forbidden
- Copyright of materials must be respected
- Posting anonymous messages and forwarding chain letters is forbidden
- As E-mail can be forwarded or inadvertently be sent to the wrong person, the same professional levels of language and content should be applied as for letters or other media
- Use of the network to access inappropriate materials such as pornographic, racist or offensive material is forbidden

Laptops

- Staff need to be aware that laptops are insured if they are accidentally or maliciously stolen by means of forced entry or assault, on school site
- If a laptop has been stolen the police need to be notified and a crime reference obtained
- Staff need to be vigilant about where they store their laptop in school
- Laptops are insured at home (see Finance Officer for details)
- Laptops should be registered on the school inventory and signed for by the staff member taking responsibility for it
- Laptops must only be connected to the internet at home through a firewall
- Laptops and hard drives/sticks should be encrypted and password locked

Ensuring Internet access is appropriate and safe

In common with other media such as magazines, books and video, some material available on the internet is unsuitable for pupils. The school will take every practical measure to ensure that children do not encounter upsetting, offensive or otherwise inappropriate material on the internet. The following key measures have been adopted to help ensure that our pupils are not exposed to unsuitable material:

- Children are taught safe ways to access information, using child friendly search engines
- Our internet access has a filtering system which prevents access to material inappropriate for children; South West Learning Grid (SWLG)/ RM must be contacted by the Computing subject lead or Class teacher if the pupils see any inappropriate sites on line in order for them to be filtered accordingly
- Children using the internet will be working in the classroom or computer suite and will be under the supervision of an adult at all times
- Staff will use their professional judgement and check that the sites pre-selected for pupil use are appropriate to the age and maturity of pupils
- Our rules for responsible internet use are posted in the ICT suite
- The Computing subject leader will ensure that occasional checks are made on files to monitor compliance with the school's Acceptable Use Policy
- Methods to quantify and minimise the risk of pupils being exposed to inappropriate material will be reviewed in consultation with colleagues from other schools and advice from the LA, our Internet Service Provider and the DfES

A most important element of our rules of responsible internet use is that pupils will be taught to tell a teacher **immediately** if they encounter any material that makes them feel uncomfortable. Pupils are asked to turn the monitor off immediately.

If there is an incident in which a pupil is exposed to offensive or upsetting material the school will respond to the situation quickly and on a number of levels. Responsibility for handling incidents involving children is taken by the Computing subject leader, the Designated Safeguarding Lead and the pupil's class teacher. All teaching staff will be made aware of the incident at a staff meeting if appropriate.

- If one or more pupils discover (view) inappropriate material, our first priority will be to give them appropriate support. The pupil's parents/carers will be informed and given an explanation of the course of action the school has taken. The school aims to work with parents/carers and pupils to resolve any issue;
- If staff or pupils discover unsuitable sites the Computing subject leader will be informed. They will report the URL (address) and content to the Internet Service Provider (SWGL); if

it is thought that the material is illegal, after consultation with the ISP and LA, the site will be referred to the Internet Watch Foundation and the police.

Maintaining the security of the school ICT network

Security is maintained by updating virus protection.

Using the Internet to enhance learning

Access to the Internet is a planned part of the curriculum that enriches and extends learning activities. As in other areas of their work, we recognise that pupils learn most effectively when they are given clear objectives for internet use.

Different ways of accessing information from the internet are used depending upon the nature of the material being accessed and the age of the pupils:

- Access to the internet may be by teacher (or sometimes other-adult) demonstration
- Pupils may access teacher-prepared materials, rather than the open internet
- Pupils may be given a suitable web page or a single web site to access
- Pupils may be provided with lists of relevant and suitable web sites which they may access
- Pupils are expected to observe the rules of responsible internet use and are informed that checks can and will be made on files held on the system and the sites they access
- Pupils will be educated in taking responsibility for their own internet access

Using information from the Internet

- Pupils are taught to expect a wider range of content, both in level and in audience, than is found in the school library or on TV
- Teachers ensure that pupils are aware of the need to validate information whenever possible before accepting it as true, and understand that this is even more important when considering information from the internet (as a non-moderated medium)
- When copying materials from the Web, pupils are taught to observe copyright
- Pupils are made aware that the writer of an e-mail or the author of a web page may not be the person claimed

Pupils are taught:

Safe surfing

Surfing the Net can be great fun, but here are some easy rules to remember that will keep you safe while you surf:

Don't give out your personal information - Don't put personal details such as your home address, telephone numbers, email address, school name

What goes online, stays online - Use privacy settings to make sure only your friends and family can see photos you post

Check your security and privacy settings - Make sure your social network privacy settings are secured so only your friends can see your personal information and use your privacy settings to restrict who can see your posts, videos and photos

Password safety - Keep your Internet passwords private and change them often. Use a hard to guess password with both CAPITAL and small letters numbers and other symbols such as: @ # ,. &.

Don't talk to strangers online- Only talk to people you actually know. Do not become friends with strangers online. Be careful making friends with people who claim to know your friends - check that somebody else knows them well before adding them to your social network.

Never agree to meet someone that you have met on the Internet.

Be wary of unsecured or unknown websites - When shopping online, use reputable and known retailers, make sure any transactions you make only take place across secure web pages which you can identify from the padlock sign in your browser address bar and where the address says https.

Use bookmarks to access your favourite websites and, if you know the web address, type it into the box at the top of the page rather than using a search engine such as Google or Yahoo. When searching for a site on Google take time to look at the website results. The first site that comes up may not be the site you are looking for. Some websites may not be genuine but may have a very similar address.

Be careful what links you click on - Avoid clicking links in an email, instant message or on your social network unless you are sure the message is from someone you know.

If you enter a site or receive information that makes you feel uncomfortable, tell someone you trust.

Always protect your mobile device - Make sure your mobile phone is pin-protected so all your personal information stored on it is safe. Download a security app which allows you to remotely wipe any personal data, should your mobile be lost or stolen

Strangers online - Learn some common tricks of online predators

Only talk to people you actually know. Do not become friends with strangers online. Be careful making friends with people who claim to know your friends - check that somebody else knows them well before adding them to your social network.

Stay 'SMART'

Safe - Keep safe by being careful not to give out personal information such as your name, email, phone number, home address, or school name - to people who you don't know or trust online.

Meeting someone you have only been in touch with online can be dangerous. Only do so with your parents or carers' permission and even then only when they can be present.

Accepting emails, IM messages, or opening files, pictures or texts from people you don't know or trust can lead to problems - they may contain viruses or nasty messages.

Reliable. Someone online may be lying about who they are, and information you find on the Internet may not be reliable.

Tell your parent, carer or a trusted adult if someone or something makes you feel uncomfortable or worried. You can report online abuse to the police at Think you know.

At School: Internet Rules

These are the rules we follow to keep us all safer on the internet when we are learning.

- ✓ **Log on with your own password**, or one that the teacher has given you.
- ✓ **Make sure** that you never give your own or anyone's details over the Internet. This includes full name, address, telephone number, email address, mobile number or photograph.
- ✓ **Make sure** that you never give the school's name unless you have permission from your teacher.
- ✓ **Never agree** to meet anyone who contacts you on the internet. Always tell your teacher if someone asks you to do this.
- ✓ **Always tell your teacher** if you see anything, which makes you feel uncomfortable. Switch off the monitor.
- ✓ **Always tell your teacher** if someone sends you a nasty message. Remember it is not your fault if you get a message like this.
- ✓ **Make sure** you only go on websites your teacher gives you permission to use.
- ✓ **Only** go on the Internet when your teacher is in the room.
- ✓ **Never download** music or programs without permission.
- ✓ **Remember** that the school may check your computer files and may look at the internet sites that you visit.

All pupils sign the pupil's AUP and staff will monitor this to ensure that they follow the school rules. See Appendix 1 below.

Using e-mail

Pupils learn how to use an e-mail application and are taught e-mail conventions. Staff and governors use school e-mail to communicate with others, to request information and to share information. Email addresses are password protected and should not be shared with others. Children must only use school email addresses to communicate with each other as part of the Computing curriculum.

- Pupils are only be allowed to use e-mail once they have been taught the rules of responsible internet use and the reasons for these rules
- Teachers endeavour to ensure that these rules remain uppermost in the children's minds as they monitor children using e-mail
- Pupils may send e-mail as part of planned lessons but will not be given individual e-mail accounts
- Incoming e-mail to pupils will not be regarded as private; emails from students should not be responded to unless on a school email account

- Children will have the e-mail messages they compose checked by a member of staff before sending them
- The forwarding of chain letters will not be permitted
- Pupils are not permitted to use e-mail at school to arrange to meet someone outside school hours

Photography

- Only school cameras, Ipads and computers will be used to take photographs of students; photographs must be downloaded at school or onto school equipment
- Parents/carers will be asked when the children start school and during any administration reviews to give permission for their child to have their photograph taken and used in a variety of contexts: on display in school; on the website; in the local press; on social media; film footage in school; films to share with classmates; film on social media and image in the National press
- Parents, carers and visitors to school are reminded about not taking photographs/films during performances and opportunities are given where possible to take photos/films of their own child

The School Website

Our school website is intended to:

- Provide accurate, up-to-date information about our school
- Follow the statutory guidance of the DfE
- Provide pupils with the opportunity to publish their work on the internet for a very wide audience including pupils, parents, staff, governors, members of the local community and others
- Celebrate good work
- Provide links to other recommended website for pupils, parents, staff, governors and supporters
- Promote the school

The point of contact on the web site will be the school address, telephone number and e-mail address. We do not publish pupils' full names or photographs that identify individuals on our web pages. Home information or individual e-mail identities will not be published. Permission will be sought from other individuals before they are referred to by name on any pages we publish on our web site.

The website address is: http://www.hestersway.gloucs.sch.uk

Social Media Sites

Pupils are taught that they should not have profiles on sites such as Facebook (must be 13 years old to have an account). Staff may have social networking profiles; however, they must not make friends with pupils and report any concerns or contact made from pupils to the Designated Safeguarding Lead. It would also be best practise not to be friends with any parents from the school due to links with the social media community; children would also be able to access information at home through the parent's profile.

Staff are not permitted to write any derogatory remarks about school on Social Networking sites.

If any pupil or parent comments on social sites are of concern, these should be reported to the Head Teacher to investigate and address.

Passwords

Staff computers should have logins, as well as email accounts. Passwords should not be shared with others. Pupils have log ins to school computers.

- Users should not logon to or use any account other than their own
- Users should always logoff when leaving a workstation, even for just a short period of time
- Hard-drives should be password protected and computers that are taken home with pupil information on should be encrypted (Our ICT company can do this please speak to the Finance/Admin Officer if you need this to be put in place)

Safer Working Practise

This policy should be used in conjunction with our safeguarding policies. In particular, the Safer Working Practise policy issued by our Local Authority on the GSCB website provides clear guidelines by which to keep children and staff safe at work.

Mobile Phones

We have a school mobile phone that will be used for school trips, residentials and any other school events. This mobile number can be given to parents/carers to contact staff if needed. Staff must not contact pupils by text or mobile phone and vice versa. Teaching staff's mobile phones should not be on view in classrooms. A member of the Senior Management Team should be informed if a member of staff is using their mobile phones in a case of emergency and that it may be on during learning or school time. No photos or films of pupils should be taken on personal devices including mobile phones. Staff are able to use their mobile phones in emergencies to safeguard e.g. making calls to other staff members or emergency services. They should limit the use of their mobile phones to their break or lunchtime. They should never share their personal phone number or details with a pupil or parents/carers.

Pupils may be given mobile phones by their parents/carers to safeguard them walking to and from school. Mobile phones should be handed into the school office during the school day to restrict unauthorised use in school. No photos or films should be taken by pupils at school.

Other policies

This policy will be used in conjunction with these policies:

Acceptable User
Allegations Management
Anti-Bullying and Hate Policy
Attendance
Complaints
Child Protection/Safeguarding Policy
Early Help Offer
E-Safety Policy
First Aid and Medication
Health and Safety

Keeping Children Safe in Education – Part 1 (most up to date version)
Lettings/Hirers agreement
Offsite Visits
SEND Local Offer
Safeguarding
Safer Recruitment and staff HR policies
Safer Working Practice
Special Educational Needs and Disabilities (SEND)
Staff Behaviour - Code of Conduct and Teaching Standards
Whistle Blowing
Working Together to Keep Children Safe

This policy was written in November 2017.
This policy was reviewed in January 2019.
It will be reviewed in January 2020.
Ratified by the Governors: _____ Date: _____

Appendix 1.

Hester's Way Primary School

Pupil Acceptable Use Agreement

I will ensure I stay safe when using technology at school by agreeing to the following:

- ✓ I will ask an adult if I want to use the computers and only use them when an adult is nearby.
- ✓ I will only use activities that an adult has told me I am allowed to use.
- ✓ I will only use ICT in school for school purposes.
- ✓ I will only open / delete my own saved files and respect others' work.
- ✓ I will ensure that all ICT contact with adults and other children is acceptable and polite.
- ✓ I will keep any ICT passwords private.
- ✓ I will not deliberately look for, save or send anything unsuitable or unpleasant.
- ✓ If I accidentally find anything unsuitable or I see something that upsets me - I will tell an adult immediately.
- ✓ If I see someone else viewing unsuitable content I will tell an adult immediately.
- ✓ I will always be sensible and responsible when using any form of ICT to keep myself safe and look after the equipment.
- ✓ I will not give out any personal details such as my name, address or phone number.
- ✓ I understand that my use of ICT can be checked at any time and that my parent/carer will be contacted if any concerns arise.
- ✓ I will only use my own personal devices in school if I have permission.
- ✓ I will not arrange to meet someone offline unless a responsible adult comes with me.

Hesters Way Primary School

Pupil Acceptable Use Agreement

Once you have read and understood the Acceptable Use Agreement please fill in the sections below to show you have agreed to follow them.

I have read and understood the Acceptable User Agreement and agree to follow them in order to help support the safe use of computing at our school. I understand that if I do not follow any of these rules my use of ICT in school may be restricted.

Name:……

Year Group:……

Signed:……