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, 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 emails sent and for contacts made that may result in email 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 emails 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 and at home.
- 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 curriculum 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 DfE.

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 curriculum 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 curriculum 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. Close the screen, turn the devise away so that children cannot see or switch off the screen on the device.
- ✓ **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 SWLG AUA and staff will monitor this to ensure that they follow the school rules.

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

There is an online safety page on our school website, with links to suggested online safety information for pupils and parents, within our Home Learning section. This refers to information from the KCSiE document – Annex C.

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 GSCP 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 Leadership 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.

Home/Remote Learning

School have set up a remote learning agreement with pupils/parents/carers, which includes Acceptable User information with regard to online learning.

Laptops loaned by parent/carers also have a clear agreement for the use of the laptops and their responsibility to keep their child safe at home, online, and report any concerns to school.

These will be updated as and when needed and is not an exhaustive list.

Remote Learning - Acceptable User

At Hester's Way Primary School, we expect everyone to be respectful and do their best to follow guidance to stay safe online. Please see our "One Line Safety" page under Home Learning https://hesterswayprimaryschool.co.uk/home-learning/#OnlineSafety and use our E-Safety Policy https://hesterswayprimaryschool.co.uk/wp-content/uploads/2020/12/E-Safety-Policy-HWPS-July-2020.pdf Please report any concerns immediately to the school leader/designated safeguarding lead. Everyone must know and understand that safeguarding everyone online is vital to protect our pupils.

It is extremely important to have positive relationships, communicate and receive feedback from our stakeholders, in order to work together effectively and continuously improve. This is done is various ways at our school.

Teaching staff with use phone calls, emails and online meetings to communicate with you and your child at home. Everyone's well-being should be considered and staff are expected to communicate only in their contractual hours, unless there is an agreement with the Head Teacher regarding staff cover, work-life balance or time management during this challenging time.

The Behaviour Policy will be followed and if pupils do not follow school rules online they will be asked not to join the meetings. https://hesterswayprimaryschool.co.uk/wp-content/uploads/2020/12/Behaviour-Policy-Sept-2020-1.pdf

Children and Parent/carers will:

- Set up new passwords when prompted and under their new account when needed; not share these with anyone. Contact school immediately if you think that someone else has access to the pupil account.
- Be aware of the Safeguarding and GDPR implications for sharing information and communicating online and report any errors or concerns immediately to the Head Teacher. See Child Protection, E-Safety and GDPR policies on the school website.
- Pupil initials should be used where possible to communicate online, please do not you're your full name then have your image on the scree – children can be traced online using this personal information.
- Use TEAMs to connect with teaching staff each other in virtual meetings; we expect everyone to use this platform sensibly and with respect for others.
- Our email system is on RMUnify.com and pupils have their own account; please do not use the pupil email for personal use.
- Classes have their own home learning emails; teaching staff use these to communicate with parents during normal school hours, this includes sending and receiving home learning, as well as answering queries.
- Any communications not related to the class and learning are forwarded to the relevant SLT, SENDCo, PST or office staff. See the school website for contact details.
- If parents/carers, or the same parents/carers overuse the communication system this will be reported to SLT to be addressed, as this could affect the well-being of staff.
- Home learning will be emailed out daily or weekly (in separate emails for each day), including power-points, links to visuals and support on Oak National Academy.
- If using websites like YouTube for Kids, parents/carers must be mindful that children can be two clicks away from inappropriate content and people, so try to use only the school approved sites. Parents/carers may wish to use other sites to support their child's learning and will be responsible for monitoring their child's safety online.
- Staff will only recommend our Home Learning Offer sites for specific learning, although other resources available to parent/carers may be shared on our school social media.
- School reserves the right to check these pupil email accounts, as per our E-safety Policy. If parent/carers receive emails from others not related to school they should report this to school immediately for safeguarding purposes.
- Class virtual meetings should have two members of staff (Teacher and TA); when teachers are in Critical Key Worker and Vulnerable groups and staffing is limited teachers will invite members of the Senior Leadership Team or Pastoral Support Team.

- Only join the meeting using camera and mic when there are two or more in the meeting (safeguarding). Pupils must leave the meeting before the staff – say goodbye and leave immediately at the end of a session. Report any concerns to SLT.
- Please use a screen background or turn the camera off for additional security – your home is a private place.
- There may be safeguarding issues seen during virtual meetings – these must be reported these immediately to the DSL via phone or email.
- Please contact your child's class teacher or the Leadership Team at school if you have any queries or concerns.

User Agreements

Users of the school systems will be given and asked to sign acceptable users agreements, including pupils, parent/carers, staff and other visitors. Reception/KS1 children will be supervised and this information verbally shared.

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
Online or E-Safety Policy (This detail acceptable user details for pupils and staff)
First Aid and Medication
Health and Safety
Keeping Children Safe in Education – Part 1 (most up to date version) and Annex - Online Safety
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 reviewed in January 2023.
It will be reviewed in January 2024.

Draft to be ratified by the Governors on 13.03.23.

Laptop Agreement Letter

Head Teacher: Kirsti Ashman
Dill Avenue, Cheltenham,
GL510ES
T 01242 525616
Ehead@hestersway.gloucs.sch.uk
www.hestersway.gloucs.sch.uk

Date

Dear Parents/Carers,

DEVICE AGREEMENT - LAPTOP

This letter confirms that a laptop has been allocated as part of the Department of Education initiative to provide pupils with access to a laptop for educational purposes. This is a school laptop and is being loaned to you for the immediate period of National Lockdown, in Spring Term 3 2021.

Entitled child/ren's name/s: _____

Year group: _____

Laptop asset number: _____

Dated: _____

Subject: Provision of laptop and related equipment

1- Department for Education has made arrangements for provision of laptops and related equipment to entitled children and young persons to enable them to continue with their education through online learning or carrying out web search relevant to their studies. The laptops have been gifted to the schools who are loaning them to the relevant children/young persons for use, in accordance with their own respective terms and procedures.

2- School has identified your child/children as needing the provision of the laptop. School reserves the right to identify and if needed, in line with safeguarding, behaviour, health and safety and the finance policies, withdraw the loan of the laptop.

3- If your child no longer needs the loan of the laptop, or leaves the school, the laptop must be returned.

4- You will be asked to return the laptop to school at times, and must do so, to enable school to use the laptops effectively. We aim to teach the children how to use the laptops in school, so that they can use them to study at home, as independently as possible.

5- The equipment is primarily to help and support in your child's studies. You may also use them for entertainment purposes in accordance with the IT policy of your school. Necessary software and filters keeping in view your requirements have already been installed to maximise your safety and benefit. Please do not save any personal information on the laptop.

6- You will be responsible for safety and security of the laptop/equipment and will only be permitted to use this for the above noted purposes. Under no circumstances will you use this equipment for any illegal or immoral purpose. Any concerns will be reported to the necessary agencies.

7- In case of any fault or trouble with the laptop or any related equipment, please refer to the school who should be able to rectify the fault and provide assistance. In the unlikely event of the school IT department not being able to rectify the fault they may escalate the matter to the DfE, as the laptop supplier.

8- Please check the equipment to ensure it is in proper working order. Should you find any fault impacting functionality of the laptop, you will be required to immediately (but not later than one week after receiving the laptop) raise any issue directly with the school who, if being unable to rectify the fault may approach the DfE for a replacement laptop or other faulty equipment.

9- As a loaned laptop, we expect the equipment to be used and treated with respect and not purposefully damaged.

10- You will be responsible for keeping your child safe online, whilst they are using the laptop. Any safeguarding concerns must be reported to the school immediately.

11- You will be responsible for the energy and broad band supply, to effectively use the laptop at home.

12- Please sign a copy of this letter to confirm that you have received the equipment and that you understand the terms of use following the intrusions below.

Yours Sincerely,
Miss Kirsti Ashman
(Head Teacher)

Online safety guide for parent/carers:

https://swgfl.org.uk/resources/online-safety-guidance-for-parents/

Desktop: Shortcuts to the necessary websites that the school uses for home learning have been added to the desktop for easy access.

Broadband or extended data offer: Schools, trusts and local authorities can request mobile data increases when schools report a closure or have pupils self-isolating. They can also make requests for children who cannot attend school face-to-face because: they're clinically extremely vulnerable; restrictions prevent them from going to school.

Please email lgreen@hestersway.gloucs.sch.uk For each request, we need to know:

- the name of the account holder
- the number of the mobile device
- the mobile network of that device (for example Three or EE)

Your information will be collated and sent to the government department working on this scheme. Once a network provider has processed a data increase, they'll send a text message to the account holder. It's also possible to check the status of requests through the online service. Network providers include: EE, Three, Sky Mobile, SMARTY, Tesco, Virgin – other may join the scheme.

Schedule: Device - Microsoft based laptop with charger in box, tick if received. Please keep and return the laptop in the box. **This signed form will remain on file, as proof of the loan.**