



HOE VALLEY SCHOOL ACCEPTABLE USE POLICY

Person Responsible	Head Teacher
Date Adopted	September 2015
Date of last review	Summer 2021
Date of next review	Summer 2023

INTRODUCTION

Hoe Valley School (HVS) aims to be a school for the 21st Century which embraces technology to support learning, information sharing and communications. This policy outlines how electronic devices will be used in an acceptable and professional way to ensure the safety and wellbeing of all staff and students. The school is a Google School and will use Google Workspace, including the Google Drive, G-mail and Google Classrooms. The School's Management Information System is SIMS.

This policy should be read alongside the **HVS E-Safety Policy, Social Media Policy** and the **Communication with Parents policy**. It also links to the Staff Handbook.

1. AIMS OF THE POLICY

An Acceptable Use Policy is about ensuring the school uses the internet, email and other technologies available in a safe and secure way. The policy also extends to out of school facilities including, but not limited to; equipment; printers and consumables; Internet and email; the Google Drive and websites.

An Acceptable Use Policy also seeks to ensure that the school community are not knowingly subject to identity theft and therefore fraud. The policy also aims to avoid cyber-bullying and abuse.

HVS recognises the importance of ICT in education and the needs of students to access the computing facilities available within the School. The School aims to make the ICT facilities it has available for students to use for their studies both in and out of lesson times. To allow for this HVS requires all students, parents and staff to sign a copy of the Acceptable Usage Policy before they receive their username and password (see appendix).

2. ACCEPTABLE USE OF EQUIPMENT

2.1 Vandalism

Vandalism is defined as any action that harms or damages any equipment or data that is part of the School's ICT facilities. Such vandalism is covered by the Computer Misuse Act 1990.

This includes, but is not limited to:

- Deliberate damage to computer hardware
- Change or remove of software
- Unauthorised configuration changes
- Create or upload computer viruses
- Deliberate deletion of files.

Such actions reduce the availability and reliability of computer equipment and puts at risk other users' data. In addition, these actions lead to an increase in repairs of the ICT facilities, which impacts upon every student's' ability to use the ICT facilities. The other result of vandalism is that it incurs costs, which reduce the funds available to improve the ICT facilities the School has. Parents/carers will be billed for any vandalised equipment.

2.2 Use of Removable Storage Media

Whilst HVS accepts the fact that you may wish to transfer school work done at home to school using a memory device, the School cannot guarantee that your work will be able to be transferred properly and safely in this way. We therefore do not allow staff or students to use removable devices with School equipment, and all sharing or transfer of documents and other resources should be done using the Google Drive.

2.3 Printers and Consumables

HVS aims to be as paper free as possible and there is limited access to printers. The Google Drive is a more efficient way to share documents.

However, when printing is required, you must use the printers sparingly and for educational purposes only. All printer use is recorded and monitored via Papercut and therefore if the printer is used for non-education or offensive material a disciplinary process will be triggered.

3. ACCEPTABLE USE OF THE INTERNET

The internet is a valuable resource for student learning, teaching resources and the day to day operation of the School. The internet should be used appropriately with your role in the School and as such use of the Internet should be in accordance with the following guidelines. Guidelines in italics apply to students only:

- Only access suitable material – the Internet is not to be used to download, send, print, display or transmit material that would cause offence or break the law
- Do not access
 - Internet Chat sites
 - Online gaming sites
 - Any site that contains sexual/ obscene content
 - Any hate groups, or discrimination websites
 - Any material that could be viewed as condoning unlawful activities.
 - Any material that relates to harassment on the grounds of race, sex, marital status, colour, ethnic or national origin, nationality, religion, disability or sexual orientation.
- *Never give or enter your personal information on a website, especially your home address, your mobile number or passwords*
- *Do not download or install software from the Internet, as it is considered to be vandalism of the School's ICT facilities*

3.1 Content Filtering

HVS believes in educating students on safe, productive use of the internet rather than continually blocking material. This is addressed via Computer Science, tutor time and PSHE lessons.

In addition to this, HVS provides internet filtering, designed to remove controversial, offensive or illegal content. The Classroom Monitoring software provides a second layer of protection. However, it is impossible to guarantee that all controversial material is filtered. If staff or students come across any inappropriate website or content whilst using the ICT equipment, they must report it to a member of SLT immediately.

3.2 Monitoring

All email and Internet access is logged and actively monitored and they are stored for up to, at least 2 months and usage reports can and will be provided to any member of staff upon request.

All Email sent on HVS accounts or devices are open to investigation by the School. For reasons of safeguarding and wellbeing HVS uses monitoring software. This

software checks all computer activity and searches for keywords and phrases that could be used for grooming or other activity that may put students at risk. This software checks all document types that are opened on school owned devices irrespective of the location of the device/.

The School will conduct e-mail sweeps, or access e-mails either at random or as part of the investigation from time to time to see if:

- the use of the e-mail system is legitimate
- to find lost messages or to retrieve messages lost due to computer failure
- to assist in the investigations of wrongful acts comply with any legal obligation.

Your inbox may be checked in the event of your absence from work due to holidays or otherwise.

4. PRIVACY AND DATA PROTECTION

4.1 Passwords

This covers all accounts for services used by the school including but not limited to; Google Workspace, Behaviour Watch, CPOMS.

- Never share your password with anyone else or ask others for their password
- When choosing a password, choose a word or phrase that you can easily remember, but not something which can be used to identify you, such as your name or address.
- If you believe that someone else may have discovered your password, then change it immediately

4.2 Security

- Never attempt to access files or programs to which you have not been granted access to. Attempting to bypass security barriers may breach data protection regulations and such attempts will be considered as hack attacks and will be subject to disciplinary action
- Wherever possible multi-factor authentication should be used on all accounts for Staff
- You should report any security concerns immediately to the IT Manager.
- If you are identified as a security risk to the School's ICT facilities, you will be denied access to the systems and be subject to disciplinary action

4.3 Storage and Safe Transfer of Personal Data

HVS holds information on all students and in doing so, we must follow the requirements of the Data Protection Act 1998. This means that data held about students can only be used for specific purposes and therefore all data will be recorded, processed, transferred and made available according to the Data Protection Act 1998. The school will seek to ensure that personal data sent over the internet will be encrypted or otherwise secured via an Egress account.

5. SUPPORT

HVS will support all staff as far as possible in terms of safely storing, recovering and saving data. The School backs up its network drives on a daily basis. It is the responsibility of all staff to save any work on the network drive regularly and to save documents in a sensible and safe way. The Google Drive instantly saves and so this is the recommended means to store data. Staff should be mindful that if the internet is not available they will not have access to web based services such as; Google Drive or SIMS.

6. PERSONAL MOBILE DEVICES

For reasons of safety and security staff and students should not use their mobile phone or any other personal mobile devices in a manner that is likely to bring the school into disrepute or risk the welfare of a child or young person. If you are sent inappropriate material e.g. images, videos etc. you should report it immediately to a member of SLT.

As part of our commitment to safeguarding and to ensure the enjoyment of parents and students at school events, the school will share photos and videos with audiences after school events. Parents are asked to refrain from using personal devices at school events for videoing or recording.

Mobile devices have features which include: picture messaging; mobile access to the Internet; video capture and streaming. Adults working within the school environment may be sent inappropriate images or videos, or be encouraged to send back images or video of themselves using integrated cameras.

Mobile phones should not be visible and be switched off during the school day. See the Behaviour for Learning / Child Protection - Safeguarding policies for further information.

The School may issue mobile phones and/or tablets to staff for use in connection with School activities. Such devices are covered by this Policy and are only to be used in direct connection with School activities - for example calling the School during a School Trip.

Staff should see the staff handbook for further information about acceptable use of email.

7. ACCEPTABLE STUDENT USE OF EMAIL

As a Google School HVS will be using Google Classrooms. Students will have access to Google Classrooms. This will be for academic and internal use only. Google classrooms allows students to collaborate on projects, receive feedback from one another and their teachers and submit work. Students should not email staff and staff should not email students. Instead, any concerns can be raised directly by contacting office@hoevalleyschool.org or by emailing dsl@hoevalleyschool.org

8. ACCEPTABLE USE OF SIMS

The school has appointed Capita SIMS to be its Management Information System (MIS) provider. Part of the MIS system supports communication internally and with parents. All of the protocols above apply to SIMS. However, it is acceptable to contact parents via the parent portal to share positive news about students only. This should not lead to an online conversation and a response from a parent requesting further information should be replied to by phone (as above).

APPENDIX ONE

ACCEPTABLE USE AGREEMENT WITH STUDENTS / PARENTS

STUDENT

I have received an electronic copy of the Acceptable Use of ICT policy.

I understand and agree to the policy. I understand that any disobedience may result in disciplinary action and the removal of my privileges to access ICT facilities. I also agree to report any misuse of the system to a staff member and I understand that misuse may come in many forms but may be viewed as any messages sent or received that indicate or suggest pornography, unethical or illegal activities, racism, sexism, inappropriate language or any act likely to cause offence.

Your acceptance of this agreement is made electronically via the link shared with you by your tutor or Head of Year when you start at HVS

PARENTS / CARERS

As the parent / carer of _____

I have received an electronic copy of the Acceptable Use of ICT policy and understand that access to electronic information services is designed for educational purposes. I understand that, whilst the Internet service provider operates a filtered service, it is impossible for Hoe Valley School to restrict access to all controversial materials and will not hold the school responsible for materials acquired while using a school device or while on the school network. The school will monitor any school owned device irrespective of location or time of day. I also agree to report any misuse of the system to the School.

I hereby give my permission to Hoe Valley School to permit my child access to electronic information services and I certify that the information given on this form is correct.

Your acceptance of this agreement is made electronically via the link shared with you when your child starts at HVS.

ACCEPTABLE USE AGREEMENT WITH STAFF, GOVERNORS AND VISITORS

I have received and read the Acceptable Use Policy and am aware of the following responsibilities:

- I understand that ICT includes a wide range of systems, including mobile phones, digital cameras, laptops and tablets
- I understand that it is a disciplinary offence to use the school ICT equipment for any purpose not permitted by the school
- I will not disclose any passwords provided to me by the school
- I understand that I am responsible for all activity carried out under my username
- I will not install any hardware or software on any school owned device without the permission and supervision of the HVS IT department , and the agreement of a member of SLT
- I understand that my use of the internet may be monitored and if anything untoward is uncovered, could be logged and used in line with any disciplinary procedures. This includes all school owned devices and isn't limited to device location or time of day. If an E-safety incident should occur, staff will report it to the Senior or Deputy Designated Safeguarding Lead as soon as possible
- I will only use the School's email / internet / intranet etc and any related technologies for uses permitted by the Head Teacher or Governing Body. If I am unsure about an intended use, I will speak to the Head Teacher beforehand
- I will ensure that data is kept secure and is used appropriately as authorised by the Head Teacher or Governing Body. No passwords should be divulged and memory sticks should also be encrypted
- Personal devices must only be used in the context of School activities with the explicit permission of the Head Teacher. Personal mobile phones or personal digital cameras must not be used for taking any photographs related to School activities
- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory
- I will only use the approved email system for school business
- Images will only be taken, stored and used for purposes within School unless there is signed parental permission for alternative use. This information is stored on SIMS
- Filming and photography by parents and the wider community at school events, such as sports days and school productions, are not allowed. When possible, a professional photographer will come to school to take photographs of students. These will then be made available to parents
- I will make every effort to comply with copyright and intellectual property rights
- I will report any incidents of concern regarding staff use of technology and/or student's safety to the Head Teacher or the Deputy Designated Professional in line with the HVS Safeguarding Policy

Your acceptance of the terms of this policy is made via CPOMS.