HAMWIC EDUCATION TRUST

ACCEPTABLE USE OF IT POLICY
Westover Primary School

Prepared By:	Name: James Anderson		
Approved By:	Name:	Date:	Date: June 2023
Start Date:	Date: June 2023	Review Date:	Date: June 2024

Contents

Introduction:

Digital technologies have become integral to the lives of children, young people and adults, both within schools and outside school. These technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. People should have an entitlement to safe access at all times.

This Acceptable Use Policy is intended to ensure:

- That people will be responsible users and stay safe while using the internet and other digital technologies for educational, personal and recreational use.
- That school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.

The school will try to ensure that everyone has good access to digital technologies to enhance their learning and will, in return, expect them to agree to be responsible users.

Terms of use

- **Responsibility**: School IT systems must be used in a responsible way, to ensure that there is no risk to your safety or to the safety and security of the IT systems and other users.
- **Monitoring**: The school will monitor use of the systems, devices and digital communications.
- **Vandalism**: Please report any cases of vandalism to the IT support team/school/Trust, and appropriate action will be taken by the school to recover any costs for loss or damage.
- **Personal use:** The school systems and devices are primarily intended for educational use and you cannot use them for personal or recreational use unless you have permission.
- **Own devices:** If allowed to use your own devices in school, you agree to follow the rules set out in this agreement, in the same way as if you were using school equipment.
- **Concerns**: If you have any concerns about the validity of an email (due to the risk of the attachment containing viruses or other harmful programmes), please inform the IT support team immediately.
- **Data security & retention**: Data is backed up daily**.** If you should accidentally delete/lose files in your folder or shared area, please inform the ICT support team immediately so that they can check if it can be recovered.
- **Protect school IT resources** by careful and considerate use of equipment and networks, reporting faults and minimising the risk of introducing computer viruses or similar to the system.
- **Protect Pupils** from harmful or inappropriate material accessible via the Internet or transportable on computer media.
- **Protect the Confidentiality** of individuals and of school matters, including complying with the Data Protection Policy and supporting documents, and not sharing sensitive or private information without authorisation, either intentionally or unintentionally.
- **Equipment Disposal:** Hamwic will dispose of all redundant ICT equipment in accordance with Waste Electrical and Electronic Equipment (WEEE) directive and the Data Protection Act 2018 (DPA). Any equipment that is to be resold must have a demonstrable audit trail to prove that is has been disposed of in line with ESFA requirements and authorisation has been sought by the same, where appropriate. We will ensure that all data is wiped prior to disposal, which could potentially mean personal data being lost

DO'S	DON'TS
• Keep usernames and passwords safe and secure	• Do not share them, or use any other person's username and password • Do not write down or store a password where it is possible that someone will steal it
• Be aware of "stranger danger", when communicating on-line	• Do not disclose or share personal information about yourself or others when online (this could include names, addresses, email addresses, telephone

	numbers, age, gender, educational details, financial details etc)
• Report any unpleasant or inappropriate material, messages, or anything that makes you feel uncomfortable when you see it online	• Do not make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work
• Respect others' work and property	• Do not access, copy, remove or otherwise alter any other user's files, without the owner's knowledge and permission
• Report any damage or faults involving equipment or software, however this may have happened	• Do not take or distribute images of anyone without their permission
• Ensure that you use any remote access systems from safe locations where you cannot compromise any sensitive information that you may need to access	• Do not try to upload, download or access any materials which are illegal or inappropriate or may cause harm or distress to others
• Lock screen if away from desk	• Do not use any programmes or software that might bypass the filtering/security systems in place to prevent access to inappropriate content
• Use secure systems for file transfers and/or sharing. Where possible keep all files stored on the school network and provide the location to the person so they can access it from there, rather than emailing the document	• Do not open any hyperlinks in emails or any attachments to emails, unless from a trusted person/organisation who sent the email
• Turn off mobile phones and hand to the class teacher on entry into school	• Do not send emails with personal details that could identify a data subject
• Disconnect or put all smart watches onto aeroplane mode. These should not be connected to any other external device or have the ability to connect to a mobile network.	• Do not forward emails to home computers or personal email addresses
	• When using social media, do not share information that can identify a data subject without permission
	• Do not use mobile phones whilst in school, this includes on the playground before or after school.

School specific systems

School IT Resources

The school will provide various IT resources within the school, including but not limited to:

- Curriculum Delivery devices (student use devices e.g. laptops, tablets, etc.)
- IT Suites

All these resources have to be used appropriately according to the terms of use laid out in this policy, the data protection policy and the equipment loan agreement.

Copyright

You may be in violation of copyright laws if you simply cut and paste material from one source to another. Most sites contain a copyright notice detailing how material may be used. If you are in any doubt about downloading and using material for official purposes, you should seek legal advice.

Printers and Consumables

All printer use is recorded and monitored and therefore if you deliberately use the printer for non-education or offensive material you will be subject to the behaviour management measures of the school.

A printer security and accounting system is in operation across the school. This facility is used to monitor staff and student use. Where students are unable to act responsibly when using the printing services, their use of these facilities will be removed. Staff must not allow students to use their codes to access the printers.

Facilities are provided in as unrestricted manner as possible to offer the best possible quality of service. It is the users' responsibility to ensure they comply with the policy.

Passwords

Access to applications and information is controlled to protect you and our organisation. It's important that the passwords you use are strong and safe enough to keep our data secure.

Choosing a secure password
When choosing your passwords:

- keep all account log in and system passwords private
- never write down your passwords or share them with anyone
- use a strong password - at least 10 characters with upper and lower case letters, numbers and special characters like asterisks or currency symbols
- Don't choose a password based on any personal data such as your name, age, or your address. Avoid using words (English or otherwise) as well as any proper names, names of television shows, keyboard sequence or anything else that can be easily guessed or identified.
- Putting punctuation marks or other symbols at the beginning or end of words is not advised either.
- For security, passwords should be a minimum of 10 characters long and contain a mixture of digits, letters and non-alphanumeric characters.

Software

- Users should use software in accordance with applicable licence agreements. It is a criminal offence to copy software or any supporting documentation protected by copyright.
- The use, or possession of unlicensed copies or "pirated" versions of software is illegal and is expressly prohibited by the school.

Network Access and Data Security

- Users must only access information held on the School's computer systems if authorised to do so and the information is needed to carry out their work. Under no circumstances should personal or other confidential information held on the school network or IT equipment be disclosed to unauthorised persons.
- If you accidentally access information which you are not entitled to view report this immediately to the Data Compliance Office and/or Data Protection Officer as a data breach.
- Students using computers in classrooms must ensure that confidential or sensitive data is not accessible to pupils or anyone else by logging off or locking the computer when away from the computer. In other areas, computers must not be left logged on when left unattended.
- Encryption: Sensitive or confidential information should be accessed via the network and should not be permanently stored on laptops or other portable devices e.g. memory sticks. Where the use of a memory stick to transfer or store data temporarily is unavoidable, this must be done using an encrypted memory stick provided by the school.

Unacceptable Use

You must not deliberately view, copy, create, download, save, print or distribute any material that:

- is sexually explicit or obscene
- is racist, sexist, homophobic, harassing or in any other way discriminatory or offensive
- contains material the possession of which would constitute a criminal offence
- promotes any form of criminal activity

- contains unwelcome propositions
- involves gambling, multi-player games or soliciting for personal gain or profit
- contains images, cartoons or jokes that may cause offence
- appears to be a chain letter
- brings the School into disrepute or exposes it to legal action

This list is not exhaustive and the School may define other areas of unacceptable use.

Breaches of Policy

Usage of school systems is subject to agreement to abide by this policy and any breach of the conditions will be dealt with, but not limited to some of the following:

- A warning
- A removal of access to services and/or devices i.e. internet, email, school computers and mobile devices
- Consequences such an official warning added to personnel file

In more serious cases or persistent breaches of this policy:

- Report to the school governors
- Report to appropriate external agencies like the police, CEOP or trade union
- Consequences such as disciplinary action for students

All students must sign and return this policy where it will be kept on their personnel file.

I understand that the school also has the right to take action against me if I am involved in incidents of inappropriate behaviour, that are covered in this agreement, or when I am out of school and where they involve my membership of the school community (examples would be cyber-bullying, use of images or personal information).	Yes / No
I understand that if I fail to comply with this Acceptable Use Policy Agreement, I will be subject to disciplinary action. This may include loss of access to the school network/internet, suspensions and in the event of illegal activities involvement of the police.	Yes / No

I have read and understood the above information.

Student Name:	Year Group:
Parent Name:	Parent Signature:
Date:	

or

Staff member:	Role:
Date	Signature: