WSS – Acceptable Use of IT Policy – Student 2023-2024

Approved by	L Paston	Date	October 2023
Next review due by			August 2024

Contents

1. 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 pupils 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. This policy aims to ensure a safe, secure, and productive IT environment for all pupils, promoting responsible digital citizenship.

2. Terms of Use

Pupils are permitted to use IT resources solely for educational purposes, research, and academic-related activities. Unauthorized access, use, or distribution of any inappropriate, illegal, or offensive content is strictly prohibited.

- **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.
- **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.
- I understand and accept that the School and Trust will fully monitor my use of the school digital technology and communications systems.
- I understand that if my activity causes any concerns, safeguarding software installed across the School and Trust may automatically alert appropriate safeguarding specialists who may choose to investigate depending on the content of the alert.
- I understand that the rules set out in this agreement also apply to use of IT technologies (e.g. iPads, laptops, email, school/Trust data etc.) out of school, and to the transfer of personal data (digital or paper based) inside or outside of the schools or Trust.
- I understand that the school digital technology systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by the Trust.
- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may access it.
- I will always lock or sign out of any device I am not actively using or will be leaving unattended and all devices under my control will require a username/password prompt or pin code before access is gained.
- I will immediately report any illegal, inappropriate or harmful material or incident I become aware of to my Tutor, a member of staff or appropriate safeguarding lead.
- I understand that if I leave the school/Trust, all my digital accounts will be suspended, and my data deleted at the School's/Trust's discretion.

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
	• Do not try to upload, download or access any materials which are illegal or inappropriate or may cause harm or distress to others
	• Do not use any programmes or software that might bypass the filtering/security systems in place to prevent access to inappropriate content

3. School Specific Systems

Email

You will be provided with an email address by the school, and the expectation is that you will use this facility for legitimate educational and research activity. You are expected to use email in a responsible manner. No messages should be sent or received if they contain any material that is sexist, racist, unethical, illegal, or likely to cause offence.

Remote Working/Access

We recognise that working offsite, or remote or mobile working, is required in many roles and situations in the school, but this brings with it a number of potential risks, to data protection, confidentiality and privacy.

The school offers remote access to pupils, and appropriate use of this technology is important.

The remote access system will enable users to access their documents and some school programs from anywhere they have internet access. Users are expected to use the remote systems in a safe and secure manner ensuring all data is kept secure and on the school storage systems for backup and compliance. School data must not be stored on any system other than issued equipment.

All issued laptops will be encrypted and the IT support team will be able to track the device when it is off the school premises.

Printers and consumables

Printers are provided across the school for use by pupils. Pupils are provided with a code/badge that they must keep private and use it to release the print jobs. You must use the printers sparingly and for school purposes only.

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.

4. 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.

5. 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.

6. 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 pupils

All pupils 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.

Staff Name:	Staff Signature:
Date:	