Whole School Policy

Policy	Acceptable Use of the School's Internet Policy			
Approval Date	Sept 2024		**Next Review**	Sept 2026
Review Cycle	**24 months**			
Scope	**Whole Group**	☐	**Whole School**	☐
	International Primary	☑	**National Primary**	☑
	International Secondary	☑	**National Secondary**	☑
Ownership	Tenby Schools, SEP		**Approved by**	SLT

Rationale

The integration of technology into the educational environment is essential for fostering a dynamic and interactive learning experience. IT facilities, including computers, networks, and digital resources, provide students and staff with powerful tools to enhance educational outcomes, promote digital literacy, and prepare students for a technologically driven world. However, the widespread access to and use of these facilities necessitates a clear framework to ensure that they are used responsibly, ethically, and in a manner that supports the educational mission of the school. The Acceptable Use Policy (AUP) is designed to safeguard the integrity and security of the school's IT infrastructure, protect the privacy and safety of users, and promote a positive, respectful digital environment.

The school's computing facilities are provided primarily for the educational benefit of students and the professional development of staff. Any behaviour that interferes with these primary objectives will be considered an infringement of Acceptable Use.

Objectives

Promote Responsible Use: To ensure that all users understand and adhere to the guidelines for responsible, ethical, and legal use of the school's IT resources, including computers, networks, and digital content.

Protect IT Infrastructure: To safeguard the school's IT infrastructure from misuse, unauthorised access, and potential security threats, ensuring that these resources remain reliable, secure, and accessible to support education and learning.

Enhance Educational Outcomes: To maximise the educational benefits of technology by encouraging the use of digital tools and resources in a manner that enhances learning, creativity, and collaboration among students and staff.

Ensure Online Safety: To protect the privacy and safety of all users by establishing clear rules for online behaviour, including guidelines on data protection, cyberbullying, and the responsible use of social media and other online platforms.

Maintain Compliance: To ensure that the school complies with relevant legal, ethical, and regulatory requirements related to the use of technology, including copyright laws, data protection regulations, and child protection guidelines.

Definitions

Computer Hardware: Any physical electronic device that is owned, operated, or managed by the school. For the scope of this policy, hardware can also relate to devices not owned by the school that are used to access our IT infrastructure under the BYOD policy.

Software: Any application that is either installed locally on a device, accessed via the school network, or deployed via cloud computing services, including software as a service (SaS).

Operating System: Any software program that provides key features of system/hardware administration including but not limited to user management, memory management, processor scheduling, and utility programs.

Network: Any hardware or software that forms part of the core IT infrastructure of the school. For the scope of this policy, this includes but is not limited to devices such as network access points, firewalls, monitoring and control systems, and any computer hardware connected to the school infrastructure.

Summary of Conditions

1. **General Policies**

- Use of computer/internet resources is for **educational purposes only**
- Access to the Internet will be supervised by a staff member
- Appropriate language must be used in all communications
- Consideration must be given to avoiding inconvenience to other computer users. E.g.) use headphones to listen to sound or music; leave computers ready for the next user to log in; do not leave programs running on computers when you leave; do not leave rubbish or paper lying around computers; replace furniture to normal positions when you leave

Students must not:

- Use abusive, racist or obscene language in any communications
- Steal, or deliberately or carelessly cause damage to any equipment
- Interfere with or change any software settings or other user's files
- Attempt to get around or reduce network security
- Logon using another user's account
- Store unauthorised types of files in their own home directories (games or other executables)
- Send "spam" (bulk and/or unsolicited e-mail)
- Reveal personal information in any communications
- Deliberately enter, or remain in, web sites containing objectionable material
- Knowingly infringe copyright
- Use VPN or similar software for any purpose including circumventing the school's filtering system

2. **Computer hardware**

Computer facilities are expensive and must be treated carefully.

Students must not:

- Do anything likely to cause damage to any equipment, whether deliberately or carelessly interfere with networking equipment
- Eat or drink near any School owned computer resources

Students must not, without permission:

- Attempt to repair equipment without permission
- Unplug cables or equipment
- Move equipment to another place
- Remove any covers or panels
- Disassemble any equipment
- Disable the operation of any equipment
- Students must also report other people breaking these rules.
- Regardless of the real or supposed levels of understanding, students are NOT authorised to attempt repair or adjustment of any college hardware or software. Any attempt will be regarded as a violation of network security. Problems with equipment or software must be reported to a teacher or technician.

3. **Software and operating systems**

Computer operating systems and other software are set up properly for computers to be successfully used in the School.

Students will not:

- Change any computer settings (including screen savers, wallpapers, desktops, menus, standard document settings, etc)

- Bring or download unauthorised programs, including games, to the school or run them on college computers, online Internet games are banned
- Delete, add or alter any configuration files
- Copy any copyrighted software to or from any computer, or duplicate such software
- Deliberately introduce any virus or program that reduces system security or effectiveness

4. **Networks**

Network accounts are to be used only by the authorised owner of the account.
It is the responsibility of students to ensure their user account details remain secure and that unauthorised use of their account does not take place.

Students must not:

- Attempt to log into the network with any username or password that is not their own
- Reveal their password to anyone. Students are responsible for everything done using their accounts, and everything in their home directories. Since passwords must be kept secret, no user may claim that another person entered their home directory and did anything to cause school rules to be broken.
- Use or possess any program designed to reduce network security
- Enter any other person's home directory (drive H:) or do anything to any other person's files
- Be logged on to the network on different computers at the same time
- Store the following types of files in their home directory:
    - Program files (EXE, COM)
    - Compressed files (ZIP, ARJ, LHZ, ARJ, TAR etc)
    - Picture files, video files, music files etc unless they are required for a school task
    - Obscene material – pictures or text
    - Obscene filenames
    - Insulting material
    - Copyrighted material
- Intentionally seek information on, obtain copies of, or modify files, other data or password s belonging to other users.

5. **Printing**

Students must minimise printing at all times by print previewing, editing on screen rather than on hard copies and spell-checking before printing.

6. **Internet usage**

The Internet use in school is not intended for entertainment.

Because the Internet is an unsupervised environment, the school has a responsibility to ensure that, as far as possible, material obtained from the Internet is not offensive or inappropriate. To this end, monitoring, recording, and filtering software is in place. it remains the responsibility of individual students to ensure their behaviour does not contravene school rules or rules imposed by parents/carers.

The school is aware that definitions of "offensive" and "inappropriate" will vary considerably between cultures and individuals. The school is also aware that no security system is perfect and that there is always the possibility of inappropriate material, intentionally and unintentionally, being obtained and displayed.

6.1 Email

Electronic mail is a valuable tool for personal and official communication both within the school network and on the Internet. Students and staff are encouraged to use it and take advantage of its special features. As with all privileges its use involves responsibilities.

Throughout the Internet there are accepted practices known as Netiquette, which should be followed. The following points should be noted:

- Use appropriate language and be polite in your messages. Do not be insulting, abusive, swear or use vulgarities.
- Never write hate mail, chain letters, harassment, discriminatory remarks and other antisocial behaviours. Therefore no messages should contain obscene comments, threats, sexually explicit material or expressions of bigotry or hate.
- Do not reveal your personal address or the phone numbers of students or colleagues.
- Note that email is not guaranteed to be private. All school emails are filtered for inappropriate content. Messages containing inappropriate content are automatically reported to the School Leadership.
- Teachers will set their own guidelines for use of email in class time.

Students will not:

- Send offensive mail
- Send unsolicited mail to multiple recipients ("spam")
- Use email for any illegal, immoral or unethical purpose

6.2 Chat lines (IRC, MIRC, IAIM etc)

Real-time chat programs (e.g. MIRC, IRC, AIM, etc) are not to be used by students.

6.3 World Wide Web

The World Wide Web is a vast source of material of all sorts of quality and content. The school will exercise all care in protecting students from offensive material, but the final responsibility must lie with students in not actively seeking out such material. It is conceivable that, especially for senior students, information is required for curriculum purposes that may appear to contravene the following conditions. In such cases, it is the responsibility of students and teachers to negotiate the need to access such sites.

Students will not deliberately enter or remain in any site that has any of the following content:

- Nudity, obscene language or sexual discussion intended to provoke a sexual response
- Violence
- Information on, or encouragement to commit any crime
- Racism
- Information on making or using weapons, booby traps, dangerous practical jokes or "revenge" methods
- Any other material that the student's parents or guardians have forbidden them to see
- If students encounter any such site, they must immediately turn off the computer monitor (not the computer itself) and notify a teacher. Do not show your friends the site first.
- The Internet must not be used for commercial purposes or for profit.
- The Internet must not be used for illegal purposes such as spreading computer viruses or distributing/receiving software that is not in the public domain.
- It is inappropriate to act as though you intend to break the law e.g. by attempting to guess a password or trying to gain unauthorised access to remote computers. Even if such attempts are not seriously intended to succeed, they will be considered serious offences.
- Interactive use of the Internet should ensure that there is no possibility of the transmission of viruses or programs, which are harmful to another user's data or equipment.
- Copyright is a complex issue that is not fully resolved as far as the Internet is concerned. It is customary to acknowledge sources of any material quoted directly and it is a breach of copyright to transmit another user's document without their prior knowledge and permission. This includes the use of images and text. It is safest to assume all content on web sites is the legal property of the creator of the page unless otherwise noted by the creator.

6.4 Penalties

More than one may apply for a given offence. Serious or repeated offences will result in stronger penalties.

- Removal of network access privileges
- Removal of email privileges
- Removal of internet access privileges
- Removal of printing privileges
- Paying to replace damaged equipment
- Other consequences as outlined in the school behaviour for learning policy