Acceptable and Responsible Use of ICT Resources Policy

Policy Lead:	**Vice Principal**
Last Review Date:	March 2023
Next Review Date:	March 2024
Approval needed by:	**Headteacher**

Introduction

The purpose of this policy is to ensure that all users of SWS's ICT network, including Internet connection, understand the way in which the all ICT resources are to be used. The policy aims to ensure that the Internet and Network are used effectively for their intended purpose, without infringing legal requirements or creating unnecessary risk.

By logging into or using any part of SWS's ICT network infrastructure, all users are agreeing to all terms and conditions of this policy.

Users will take complete responsibility for the security of their network password. If any abuse of the rules concerning network use takes place under their user name, then they will accept the consequences.

Remember that access is a privilege, not a right,
and inappropriate use will result in that privilege being withdrawn.

Policy statement

SWS encourages users to make effective use of the Internet and computer network. Such use should always be lawful and appropriate. It should not compromise SWS's information and computer systems nor have the potential to damage SWS's reputation.

Please read this policy carefully as you will be deemed to be aware of its contents.

Use of Internet and computer network facilities

SWS expects all users to use the Internet and computer network responsibly and strictly according to the following conditions.

Users shall not:

- Visit Internet sites, make, download or pass on material, remarks, proposals or comments that contain or relate to:
  - Pornography (including child pornography)
  - Promoting discrimination of any kind
  - Promoting racial or religious hatred
  - Promoting illegal acts
  - Attempt to bypass SWS's Internet content filtering solution (Smoothwall)
  - Participate in on line chat rooms or connect to any social networking sites, i.e. Facebook, Twitter
  - Any other information which may be offensive to Students and Staff including photographs and videos

Incidents which appear to involve deliberate access to Web sites, newsgroups and on line groups that contain the following material will be reported to the Police:

- Images of child abuse (images of children, apparently under 16 years old) involved in sexual activity or posed to be sexually provocative
- Adult material that potentially breaches the Obscene Publications Act in the UK
- Criminally racist material in the UK
- Any other illegal activity

Users shall not:

- Attempt to, or use other user's login accounts
- Share personal login account information with others
- Leave a machine logged on and unattended
- Attempt to gain administrative access to the School's network
- Attempt to gain unauthorised access to other equipment on the network
- Engage in activities such as password cracking or vulnerability testing
- Attempt to disrupt use by other users, e.g. by deliberately wasting network resources
- Attempt to store music, media or any other files where copyright issues may be of concern
- Upload, download, install, or otherwise transmit (make, produce, save or distribute) commercial software or any copyrighted materials belonging to third parties
- Reveal or publicise confidential information, which includes but is not limited to: financial information, personal information, databases and the information contained therein, computer/network access codes, and business relationships
- Intentionally interfere with the normal operation of the Network/Internet connection, including using Safe Mode, the broadcast of computer viruses and sustained high volume network traffic (sending and receiving of large or small files or any activity that causes network congestion) that substantially hinders others in their use of the Internet, or ICT network
- Access or open any other item they know to be gained inappropriately
- Physically damage any equipment

Users shall:

- Only use the computers for educational purposes. Activities such as buying or selling goods are inappropriate.
- Always check files brought in on removable media (such as CDs, Memory Sticks etc) with antivirus software and only use them if they are found to be clean of viruses.
- Not connect personal mobile equipment (e.g. laptops, tablet PCs, PDAs, mobile phones, etc) to the network either wired or wireless without permission from the ICT Services Team.
- Protect the computers from spillages by eating or drinking well away from the ICT equipment.

Security and Privacy

- There are systems in place for keeping students safe from extremist material when accessing the internet in our school by using effective filtering and usage policies
- Securus Forensic Monitoring software is installed to monitor all activity on the schools Network.
- Home directories, shared drives, school email accounts and memory sticks will be treated like school lockers. Staff may review your files and communications to ensure that you are using the system responsibly at any time without notification. All activity is monitored during use.

Email

- Be polite and appreciate that other users might have different views from your own. The use of strong language, swearing or aggressive behaviour is as anti-social on the Internet as it is on the street.
- Only open attachments to emails if they come from someone you already know and trust. Attachments can contain viruses or other programs that could destroy all the files and software on your computer and the school network.
- If you receive an email containing material of a violent, dangerous, racist, or inappropriate content, always report such messages to a member of staff. The sending or receiving of an email containing content likely to be unsuitable for children or schools is strictly forbidden.

Please read the above document carefully. You will be prompted at set intervals to accept the AUP when you log onto the network. If you decline you will be logged off. If you violate these provisions, access to the Internet and or computers will be removed and you will be subject to disciplinary action. Additional action may be taken by the school in line with existing policies regarding school behaviour. For serious violations, suspension or expulsion may be imposed. Where appropriate, police may be involved or other legal action taken.

Students are not allowed to use (upload, download or access) any form of data or information (including pictures and videos) of any description from any form of mobile or handheld device (mobile phone, media player, PDA etc) in school. Existing policies regarding behaviour will be enforced.