SSAL CHANGING LIVES THROUGH LEARNING

Name of Policy / Strategy:	**Acceptable Use Policy (AUP)**		
Written by:	Finance & Resources Manager		
Approved by:	CEO	**Date:**	November 2024
Implementation Date:	01/09/2021		
Review date*:	November 2027		
This document will be reviewed every 3 years or when there are operational or legislative changes that require a review.			
Associated policies, procedures & Strategies:	Remote Access Policy		
Amendments (include date) **Nov 24** **Nov 24**	Removed EBS and added TERMS from online services list Changed Twitter to X		

Acceptable Use Policy (AUP)

Purpose

The aim of this policy is to ensure that SS&L’ s IT facilities and services are used safely, lawfully and decently. SS&L’ s IT infrastructure, systems and services are provided for academic and business purposes in the interests of the organisation, for example, to support learning or in connection with employment by SS&L.

It is the responsibility of every IT user to read and comply with this policy, along with any other applicable SS&L policies and procedures, and appropriate UK and international laws. Infringements and breaches of the policy may result in disciplinary or legal action. This policy does not form part of any employee’ s contract of employment and SS&L may amend it at any time.

Scope

This policy applies to anyone using SS&L’ s IT facilities and services. In addition to SS&L staff and learners, this may include:

- External partners, collaborators and contractors working onsite and using the SS&L network, or offsite and accessing SS&L systems
- Visitors using the SS&L Public WiFi
- Visitors using a guest account to access SS&L facilities
- Visitors to the SS&L website and people accessing online services

The term IT facilities and services includes:

- IT hardware that SS&L provides, such as PCs, laptops, tablets, mobile phones and printers.
- Software that SS&L provides, such as operating systems, office software, web browsers etc.
- Access to the network provided by SS&L. This covers both the corporate in-house network and the public access WiFi
- Online services arranged by SS&L, such as Office 365, email, TERMS, Learning Assistant etc.

Unacceptable Use

The use of SS&L’ s IT infrastructure, systems and services for any activity, which may reasonably be regarded as unlawful, is not permitted.

SS&L has a duty, under the Counter Terrorism and Security Act 2015, termed ‘PREVENT’ to have due regard for the need to prevent people from being drawn into terrorism. Staff, learners and visitors using SS&L IT facilities must not create, display, download, store, transmit or distribute any unlawful material, or material that is offensive, threatening, discriminatory or extremist.

SS&L reserves the right to monitor or block access to such material. If a member of the SS&L community believes they may have encountered such material, they should report this immediately to the designated Safeguarding Officer.

In addition, SS&L’ s IT and network facilities must not be used for any of the activities described below (the list should not be taken as exhaustive):

- Creation, display, download, storage, transmission or distribution of:
    - any pornographic, offensive, obscene or indecent images, data or other material, or any data capable of being resolved into obscene or indecent images or material
    - material which is discriminatory, offensive, derogatory or with the intent to cause fear, alarm, annoyance, inconvenience or anxiety
    - material which encourages terrorism or extremism
    - material with the intent to defraud
    - false or defamatory material
    - material that infringes the copyright of another person or organisation
    - material containing confidential information about SS&L, its employees or learners unless in the proper course of duties or studies
    - malware, viruses or any other harmful component
- Wasting IT resources, interfering with IT hardware or attempting to download, import or install unauthorised software
- Attempting to gain unauthorised access to facilities or services

Personal Use

SS&L allows reasonable personal use of its IT facilities and services as a privilege, not a right, on the understanding that personal use:

- is lawful and complies with SS&L’ s rules, regulations, policies and procedures
- is not detrimental to the main purpose for which the facilities are provided
- does not interfere with the performance of an individual's duties or learning responsibilities
- does not take priority over an individual's work or learning responsibilities
- is not excessive in its use of resources
- is not for any form of personal financial gain
- does not incur unwarranted expense for SS&L
- does not in any way have a negative impact on SS&L’ s reputation

Behaviour

Real world standards of behaviour apply online and when using social networking platforms, such as Facebook, Instagram and X. When using the IT facilities, users should be mindful of the content of electronic messages or posts, including those on social networking sites, forums and virtual learning environments.

Electronic messages and posts will be read by others and deletion of posted content does not mean that an electronic message or post is irretrievable. Messages and posts should be drafted with care and convey the same courtesy and respect as when speaking face to face.

The following activities are not permitted:

- Posting of extremist, obscene or offensive comments, profanity and expletives, or otherwise objectionable material (including but not limited to unlawful, defamatory, derogatory, racist, sexist, homophobic, harassing, harmful, abusive, threatening, or sexual references)

Security

Users are responsible for the security of the equipment allocated to or used by them, and must not allow it to be used by anyone other than in accordance with this policy.

Users are responsible for the security of any computers or equipment they log into. Computers should be locked or logged off when left unattended and switched off when leaving the office/classroom at the end of the day.

All reasonable precautions must be taken to secure any personal data stored or transmitted digitally and to safeguard any IT credentials issued, i.e. usernames, passwords, PIN numbers etc. Users must not attempt to obtain or use anyone else' s credentials or share their own credentials with anyone else, no matter how convenient and harmless it may seem.

Be aware of Phishing attempts. If a password breach is suspected, the at-risk password must be changed immediately and the matter reported to PC Comms. Any suspect emails or queries over online activity must also be reported as soon as possible.

Default passwords, such as those created for new employees when they start or those that protect new systems when they' re initially set up, must be changed as quickly as possible.

Obvious passwords such as birthdays and spouse names etc. must be avoided. Passwords should exceed 12 characters and be comprised of letters [UPPERCASE and lowercase], numbers and punctuation characters.

Use common sense when choosing passwords. Avoid basic combinations that are easy to crack. For instance, choices like "password1" or "Pa$$w0rd" are equally bad from a security perspective.

Do not use the same password for multiple uses, either at work or at home. The use of password management software is highly recommended.

Passwords should be memorable. Avoid writing them down and keeping them near your password protected equipment. If you must write them down, then they should be stored securely away from the associated equipment.

Wherever possible, 2FA (two factor authentication) / MFA (multifactor authentication) should be used to increase security.

If you suspect that your device has been infected by a virus or malware, disconnect the device from the network and contact PC Comms immediately.

Portable equipment, such as laptops or mobile phones, must be kept secure at all times, especially when travelling. Passwords or PIN numbers must be used to secure access to ensure that confidential data is protected in the event of loss or theft. Users should also be compliant with the Remote Access Policy when using equipment away from the workplace.

Monitoring

SS&L monitors and records the use of its IT facilities and services, including any permitted personal use, for the purposes of:

- The effective and efficient planning and operation of the IT facilities
- Detection and prevention of infringement of SS&L policies and regulations
- Safeguarding children and young people and the need to prevent people being drawn into radicalisation or extremism (Prevent Duty)
- Complying with any legal obligations
- Investigation of alleged misconduct

Monitoring is only carried out to the extent permitted or as required by law and as necessary and justifiable for the purposes set out above. However, SS&L IT facilities are provided for academic and business purposes. There should be no expectation of privacy in any communication sent or received using SS&L IT facilities, whether it is of a business or personal nature.

All files or emails are scanned electronically for viruses, SPAM and other unwanted content. These files may be opened and interrogated should a virus or suspicious content be found.

SS&L will comply with lawful requests for information from government and law enforcement agencies.

Liability

In using the SS&L IT facilities and/or services each user agrees that SS&L shall have no liability for the loss or corruption of any user file or files, information or data; and/or the loss or damage to any user owned equipment, devices, systems resulting from the individual's use of SS&L' s IT infrastructure and services.

SS&L shall not in any event be liable for any damages, costs or losses (including without limitation direct, indirect, consequential or otherwise) arising out of, or in any way connected with, the use of these services, or with any delayed access to, or inability to use these services.

Infringement

Breaches of the Acceptable Use Policy by staff will be handled in accordance with the SS&L Disciplinary Policy and in serious cases, may be treated as gross misconduct leading to summary dismissal. Breaches by learners will be dealt with appropriately and may result in the suspension or termination of services without warning, or disciplinary action. All other users may have their access revoked.

Reporting to other authorities

If SS&L believes that unlawful activity has taken place, it will refer the matter to the police or other enforcement agency.