Skills and Training Services (STS)

Local Operating Procedure

Acceptable Use Policy

Version Control Sheet

Document Title	Acceptable Use Policy
Author	Mike Hampton
Owner	Mike Hampton
Doc version/status	V1.0
Date issued	30/10/2023
Renewal Date	30/10/2024

Version History

Version	Date	Summary of changes
V1.0	30/10/2023	First Issued

Approval

Name	Job Role	Date	Signature
Mike Hampton	Quality Improvement and Audit Manager	30/10/2023	M. Hampton

Change Control

Any requested changes to this document should be emailed to: mike.hampton@serco.com

Contents

Introduction

The term “learner,” within this policy, is used to describe all learners and apprentices involved with Skills and Training Services, this also includes those learners enrolled with subcontractors.

All Skills and Training Services staff must have read the Serco Acceptable Use of Information Systems Policy as part of their induction SMS-GS-BC1_Acceptable-Use-of-Information-Systems.pdf (serco.com). Further information can also be found on the externally facing mycode website: Using our systems toolbox | mycode | Serco. This policy aims to compliment the Serco wide policy (above) and is aimed at learners and employers. Serco staff must ensure they follow the Serco wide policy (above).

This policy sets out the behaviours that are required and the rules that must be followed by learners/employers when using the Serco information systems.

This policy must be read in conjunction with the following policies:

- Safeguarding Policy
- Online Safety Policy
- Behaviours, Disciplinary and Expectations Policy

Acceptable Use

When using Serco issued laptop/PC/equipment, Learners and employers will not:

- use removable media, such as memory sticks and portable hard drives, unless approved by Serco first, as these will require a Serco approved level of encryption.
- Intentionally introduce malicious programmes, such as viruses and trojans, into the Serco systems.
- Create computer viruses or monitor or intercept network traffic.
- Remove or disable installed anti-virus software and malware controls.
- Attempt to crack or capture passwords or decode encrypted information.
- Leave their workstation without firstly locking their equipment to prevent any unauthorised access.

Learners and employers will not use the Serco systems connected to the internet to:

- View, create, amend, distribute, transfer, store or print information that is pornographic, obscene, indecent, hateful, defamatory, or offensive.
- Engage in any form of illegal activity, including fraud, plagiarism, forgery, any form of intimidation or harassment.
- Participate in online gambling, or for soliciting personal gain or profit.
- Download, store, copy or transmit the works of others (including software, games, music and video files), without their permission, where this infringes copyright or otherwise contravenes the owner or licensor’s terms and conditions regarding permitted use.

Learners and employers will follow these principles when permitted to access social media when using the Serco systems:

- Any Serco owned materials may only be published on social media/networking (such as Facebook, YouTube, Instagram, WhatsApp, LinkedIn, Twitter, blogs, wikis, newsgroups, and any other site where text can be posted) upon prior approval from Serco first.

- They must not use social media/networking to harass, bully, threat, discriminate or be offensive or intimidating towards employees of Serco, other learners/employers or other third parties.
- They must not engage in any illegal activity or engage in any activity that promotes terrorism.
- Information must not be published that compromises the security of Serco staff, learners/employer or other third parties.

Learners and employers will follow these principles when using email/messaging services when using the Serco systems:

- Learners/employers are responsible for any content, including text, audio, images) that are sent when using the Serco systems.
- Material that is pornographic, obscene, hateful or defamatory, or intended to harass or intimidate any other individual will not be sent when using the Serco systems.
- Serco systems will not be used to generate unsolicited messages, including the sending of junk mail or other advertising material to individuals who have not specifically requested such material.
- Spam email and messages will not be replied to or forwarded to any other individual, they often contain malicious content or harmful links.

Learners and employers will follow these principles on keeping information secure via passwords when using the Serco systems:

- All passwords assigned for the use of Serco information systems will be kept safe.
- User identity or passwords or any other access code must not be written down, displayed or disclosed to any other individual.
- Users must not access information with a user identity or password which is not their own.
- If learners/employers have suspicion that their password has been compromised, they must report this to the contacts listed in the 'Reporting Misuse' section and change their password as a matter of urgency.
- Passwords that are created must be secure and follow the principles as outlined on each system being used. In general, the below should be considered:
    - Minimum length of 10 characters in length
    - Previous passwords should not be re-used.
    - Different passwords should be used across Serco systems and personal accounts.
    - Passwords must not be easily guessable, for example a birthday or child's name.
- Digital signatures must not be used that belong to another person without their consent.

All information created will be fair and will respect all religions, political, economic and racial differences and opinions and show proper consideration for others' privacy.

Reporting Misuse

If a learner/employer receives any materials, or observes an event, that contravenes the statements in this policy, this must be reported to any of the Skills and Training Services Senior Management Team as a matter of urgency.
Head of Skills Delivery: dean.hooton@serco.com
Head of Contracts: rob.matts@serco.com
Business Assurance Manager: joanne.wood@serco.com
Quality Improvement and Audit Manager: mike.hampton@serco.com

Consequences of Misuse

Non-compliance with this policy may result in disciplinary action. This can include:

- A verbal or written warning of the conduct.
- Removal of access to Serco systems.
- Reporting to the Police, in instances where the act is illegal.
- Removal from the programme of study.