



POLICIES & PROCEDURES

Acceptable Use Policy

Policy Owner:	Director of Corporate Services
Date Approved:	19 November 2025
Version:	V3.0
Equality Screening Date:	Previously completed
Date of First Issue:	September 2008
Date of Next Review:	August 2028
Location:	Staff/Student Gateway

CONTENTS

1.	Introduction.....	2
2.	Policy Scope.....	2
3.	Acceptable Use	2
4.	Unacceptable Use	3
5.	Personal Devices (BYOD)	4
6.	Monitoring.....	4
7.	Policy Acknowledgement.....	5
8.	Review.....	5
	Appendix 1: User Login Acceptance	6
	Related Documentation	7
	Change Log.....	7
	Communication	7
	Document Development.....	7
	Approval Dates.....	7
	Document History.....	8

1. Introduction

- 1.1 It is essential that all College IT systems, networks and digital resources are used appropriately. This policy outlines acceptable and unacceptable use and is in place to protect the integrity, confidentiality and availability of IT Systems, data and users.

2. Policy Scope

- 2.1 The Policy applies to all users who access, use or manage IT facilities which includes, but is not limited to:

- Desktops, laptops, tablets and mobile devices.
- Internet services.
- Learning Management Systems e.g. Canvas.
- Email and messaging platforms e.g. Outlook, Teams.
- Printing devices, photocopiers and storage devices.
- Software applications, databases, cloud services and licenced content.
- Internal networks and servers.

3. Acceptable Use

3.1 All users are expected to:

- Use IT facilities for academic or administrative purposes which are compatible with the Joint Academic Network (JANET) and current legislation.
- Keep passwords and login details/credentials confidential.
- Respect the privacy, rights and work of others.
- Comply with copyright regulations and licencing agreements.
- Protect personal and College data in line with data protection laws i.e. GDPR.
- Report any suspected Cyber-security incidents, technical vulnerabilities, breaches, inappropriate content, suspected misuse, immediately via logging a ticket on SWC Service Desk.
- Report any changes in IT requirements or IT requests via logging a ticket on SWC Service Desk.

- Follow instructions regarding use of IT facilities.
- Store/save data to their OneDrive, which is backed up and is accessible on campus and remotely. Data saved to other locations will be permanently removed during the annual reimaging process.
- Use USB facilities in exceptional circumstances only; the College may withdraw this facility at any time for security reasons.
- Use College Email for College business only.
- Use IT resources/equipment with care, avoiding eating and drinking, respecting others working in same location, maintain low noise levels.
- Fully cooperate with any investigation involving IT resources you have used.

4. Unacceptable Use

4.1 The following activities are strictly prohibited:

- Accessing, creating, sharing or distribution of offensive, illegal, discriminatory or inappropriate material e.g. pornographic, racist materials. The College may reserve the right to refer the matter to relevant authorities.
- Engaging in cyber bullying, harassment, intimidation or any online behaviour that harms others or the College in any way.
- Using IT resources for any unethical purpose.
- Attempting to access/hack another user account or system either internally or externally.
- Sharing or using another person's login credentials or accessing their accounts.
- Misrepresenting yourself as someone else i.e. via messages, phishing related activities.
- Plagiarism or any misuse of digital resources to gain unfair advantage.
- Attempting to bypass security controls, firewalls or access restrictions.
- Installing unapproved or unlicensed software, hardware or modifying any system configurations/settings as set by IT Services staff.
- Intentionally introducing viruses, malware, ransomware or any other malicious software or harmful programs to the College network.

- Storing or communicating confidential information without proper authorisation or encryption.
- Reproduction, distribution, streaming, downloading and sharing of copyrighted material without appropriate permission.
- Purchasing IT resources. IT Services manage the requisition, procurement and distribution of all IT resources.
- Use IT facilities for personal commercial gain, political campaigning or personal profit.

5. Personal Devices (BYOD)

- 5.1 All users must ensure that any personal device used to access College systems are;
- Secured with appropriate measures including strong passwords or PINs, biometric authentication where applicable, up to date software and protection from viruses or malware.
- 5.2 Users must not share access to any of their College accounts.
- 5.3 Users may access College Wi-Fi i.e. Eduroam.

6. Monitoring

- 6.1 The College reserve the right to monitor and audit the use of IT facilities to;
- Ensure compliance with this policy.
 - Safeguard users and data.
 - Investigate suspected violations.
- 6.2 Breaches and violations of this policy may result in;
- Revocation of IT access.
 - Disciplinary action.
 - Reporting to appropriate authorities if illegal activity has been identified.

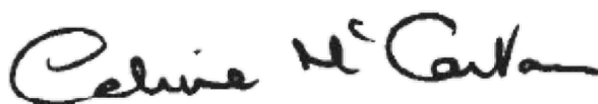
7. Policy Acknowledgement

- 7.1 When logging into the College network, users are presented with a summary of the Acceptable Use Policy and must acknowledge and comply with its terms as a condition of access.

8. Review

- 8.1 This policy will be reviewed every three years or earlier dependent on organisational necessity.

Signed Principal and Chief Executive:



Date:

19.11.25

Signed Chair of the Governing Body:



Date:

19/11/2025

Appendix 1: User Login Acceptance

SOUTH WEST COLLEGE ACCEPTABLE USE POLICY

South West College provides ICT services under license from the Joint Academic Network (JANET). All users must use these services responsibly and in line with this policy and current legislation.

Compliance

- This policy applies to all users of College ICT system.
- Breaches may result in College disciplinary action and may also violate criminal or civil law resulting in further action.

Account Access and Security

- ICT access is authorised via line manager or induction process.
- Each user is responsible for maintaining the security of their password and for all activity conducted using their account.
- Users must not access accounts assigned to others.

Monitoring

- All accounts are monitored continuously.
- Any violations of the Acceptable Use Policy are automatically detected and logged.

Internet and ICT Use

- Internet access is primarily for official College business and curriculum- related activities.
- Personal use of the internet should be limited to periods outside of working hours, such as lunch breaks.

Responsibility

All staff, students and users must acknowledge and comply with College IT policies.

Related Documentation

Title	Location	Owner
Information Security Policy	Staff Gateway	Director of Corporate Services
Information Governance Policy	Staff Gateway	Director of Corporate Services

Change Log

Location	Change from deletion/addition	Change to
	Original policy rewritten/updated to reflect current practices	

Communication

Who needs to know (for action)	Head of IT Services
Who needs to be aware	All Staff, Students, Funders, Stakeholders Governing Body, Visitors

Communication Plan

Action	By Whom	By When
Upload to Gateway and Website	Executive Support Officer	On approval
Circulation to key staff	Executive Support Officer	On approval

Document Development

Details of staff who were involved in the development of this policy:

Name	Role
Sharon McGrath	Director of Corporate Services
Paul Wade	Head of IT Services
Pamela Corrigan	Information Security Officer

Details of staff, external groups or external organisations who were consulted in the development of this policy:

Name	Organisation	Date
N/A	N/A	N/A

Approval Dates

Approved by	Date
Governing Body	19 November 2025

Document History

Issue no. under review	Date of review:	Persons involved in review	Changes made after review? Yes/No If Yes refer to change log	New Issue No.	If changes made was consultation required?	If changes made was Equality Screening required?
V0.1	September 2008	Not previously stated	Not previously stated	V1.0		
V1.0	30.08.2022	PC/PW/JL/SMcG	Yes	V2.0	No	
V2.0	06.08.2025 / 26.08.2025	PC/PW	Yes	V3.0	No	