POLICIES & PROCEDURES

Electronic Communications Policy

(Replaces the Internet, Email Usage and Monitoring Policy)

Policy Owner:	Director of Corporate Services
Date Approved:	20 November 2024
Version:	V1.0
Equality Screening Date:	December 2023
Date of First Issue:	December 2024
Date of Next Review:	December 2026
Location:	Gateway

CONTENTS

1. Policy Statement

1.1 College electronic communications are essential to support the teaching, learning, research, and approved business activities of the College. Communications sent or received via College systems form part of the official records of the College; they are not considered private property and all information contained in electronic communications will be disclosed if required.

1.2 All staff, students and anyone granted access to College systems (collectively referred to as “users”) are considered representatives of the College and they must uphold the reputation of the College. Unauthorised communications and personal opinions that are publicised and linked to College systems, can incorrectly be deemed as the College’s official position.

2. Policy Scope

2.1 This policy applies to all forms of electronic communications including but not limited to:

- Outlook Email
- Teams messaging
- Canvas
- EbS
- SMS
- Social media platforms

2.2 The policy applies to all users of College systems.

3. Policy Purpose

3.1 This policy outlines what is considered best practice when using College electronic communications. Detailed guidance on the use of electronic communications is

provided in the Appendices attached to this policy and which are a constituent part of this policy. All users are expected to be compliant with the guidance provided.

3.2 This policy replaces the Internet and Email Usage and Monitoring Policy.

4. User Responsibilities

4.1 It is the user's responsibility to familiarise themselves with this policy and the guidance provided in the Appendices.

4.2 All users are responsible for their username and password and must only log on to College systems using their own credentials. Users are responsible for all activity which is initiated under their username and therefore should ensure that no other person has access to their account.

4.3 System security is a priority of the College, and all users are required to remain vigilant regarding potential Phishing attacks.

4.4 Users must complete annual training in Phishing and any other training required or mandated by the Head of IT Services.

4.5 Users should understand that all information that they store, send, or receive via College electronic communications systems is not their private property. All activity is logged and can be traced back to individual users if necessary to permit enquiries or to support disciplinary procedures.

5. College controls on the use of electronic communications

5.1 Email addresses will be allocated to each staff member or enrolled student and will be based on usernames i.e. firstname.surname@swc.ac.uk in line with the User Account Management Policy.

5.2 Specific email addresses will be supplied on request for individual, or group use if there is a business justification.

5.3 IT Services will apply configuration settings in order to protect IT systems and attempts must not be made to modify the settings.

5.4 IT Services can be granted temporary access to users' email accounts via formal request for permission from HR Manager.

5.5 All activity will be logged and audited to protect users and the College, and all activity can be traced back to individuals.

5.6 The College will implement Multi Factor Authentication (MFA) to provide an additional level of security to the College and users.

5.7 All emails will be scanned for malware and viruses and will be blocked or quarantined if anything suspicious is found to be present.

5.8 Appropriate measures will be taken to ensure that all software used for virus/malware scanning is regularly updated.

5.9 Automatic forwarding of emails will be turned off.

6. Abuse of College electronic communications

6.1 The College has a reasonable expectation that users will not abuse the communication platforms provided for teaching, learning and general business activity and will not tolerate any form of abuse on any platform.

6.2 The College prohibits the following activities deeming them to constitute abuse:

- The use of College communications systems to conduct personal businesses activities.
- Transmitting unsolicited commercial or advertising material.

- The creation or transmission of material which brings the College into disrepute.
- The unauthorised transmission of confidential material concerning the activities of the College.
- Distribution of material which may infringe on the copyright of another person, including intellectual property rights or the copyright of materials used for learning purposes within the College.
- The creation or transmission of any offensive, obscene, or indecent images, data, or other material.
- The creation or transmission of material which is designed or likely to cause annoyance, inconvenience, or anxiety.
- The creation or transmission of material or online chat that is abusive or threatening to others, serves to harass or bully others, discriminates, or encourages discrimination on racial or ethnic grounds, or on grounds of gender, sexual orientation, marital status, disability, political or religious beliefs.
- The invasion of other Staff and Students' privacy, including distribution of private materials to other unauthorised individuals.
- Creation or distribution of anonymous messages, deliberately forging of messages or email header information (i.e., masking the original sender), or 'flaming' (i.e., sending angry or offensive email messages). If any user receives an email with inappropriate or prohibited content from any source, they should report the incident to their Line Manager/Lecturer immediately.
- The use of College email for subscribing to websites that are of personal benefit or general types of personal subscription. Inappropriate websites such as gambling and pornography must not be viewed or subscribed to using College email accounts.
- The linking of College email addresses to domestic billing accounts in the home, or for personal banking.

7. Data Protection and Freedom of Information

7.1 The College is bound by Data Protection and Freedom of Information legislation and will make every effort to ensure that the use of its electronic communications platforms is compliant with legislation.

7.2 The College requires users to carefully consider the content of any email, Teams chat and social media posts to avoid revealing confidential or personal information bearing in mind that information contained on these platforms may be discoverable if the College receives requests for information under the legislation.

7.3 Users must avoid:

- Using names in the subject heading of an email.
- Sending personal data as an unprotected attachment or in the body of an email.
- Re-sharing or forwarding information that you may have received from a third party which may have contained identifying information about an individual.
- Unnecessary printing of emails. If this is necessary, the email must be disposed of in confidential waste bags or cross-shredded if it contains confidential or sensitive information.
- Making content on their device screens visible to unauthorised persons when on site and when working remotely.

7.4 The guidance provided in the Appendices will equip users to use electronic communications in compliance with legislation.

8. Hybrid Working / Remote Access

8.1 The College promotes and supports hybrid working in line with the sectoral Hybrid Working Framework. Staff who are permitted to participate in the hybrid working arrangements, must comply with this policy and the Hybrid Working Framework.

9. Online Incidents

9.1 The College will fully investigate any complaints that are received from internal or external sources regarding inappropriate use of electronic communications, which can be linked to a College account or any College equipment.

9.2 Incidents must be reported to IT Services as soon as possible, to permit retrieval of material from the systems for the investigation. If appropriate the Data Protection

Officer will be informed and all departments will be required to support the investigation.

9.3 Dependent on the nature of the incident, appropriate measures will be taken, such as disciplinary action, police involvement and, where necessary, IT Services will prevent any continuation of the incident by disabling the user(s) device(s) and/or account(s).

9.4 IT Services will assist with the retrieval of material which may be required for the investigation.

10. Non-Compliance

10.1 All users are expected to comply with this and all related College policies and procedures. Non-compliance can result in the following actions being taken:

- Disabling of their College user device and/or account.
- Disciplinary action that is dependent on the type of non-compliance and as outlined in the Staff and Student Handbooks.
- Civil or Criminal Prosecution under UK or International Law.

11. Monitoring and Review

11.1 This policy will be reviewed every three years or sooner if legislation, developments in technology and electronic communications demand or at the College's discretion.

Signed Principal and Chief Executive: 

Date: 20.11.24

Signed Chair of the Governing Body: 

Date: 20/11/2024

Appendix 1 – Guidance for users on the acceptable use of email

1. Email protocol

- Always ask yourself whether email is the appropriate way to communicate and consider other option e.g. Teams, telephone call, face to face.
- Unless urgent, refrain from sending emails outside of normal business hours.
- Always use your College email address when using email for College business.
- Communication between staff and students must always be via College email addresses not personal email addresses.
- You should check that the email is written in a manner that is professional and courteous.
- Be clear, concise, and respectful.
- Proofread your email and pause on send if you need to check your emotions.
- Avoid the use of capital letters, red text, or lots of exclamation marks.
- You should be wary of predictive text and check that the email address you intend to send the email to is correct.
- Always use a subject line. Choose an appropriate description avoiding the use of names or anything that might identify an individual.
- Carefully consider the use of BCC, CC, and Reply All:
    - BCC when you need to be discreet or protect the privacy and personal information of recipients.
    - CC only the individuals who need to receive your reply.
    - Reply-All only when everyone in the email thread needs to see your response.
- You must not attach documents containing personal information unless the document is password protected. The password must be sent in a separate email. If you are required to share personal information, it is advised to use a private Teams channel.
- Do not forward College business emails to any personal accounts.
- If you are unavailable to reply to emails, set an Out of Office automatic reply and, wherever possible, provide information as to when you will return and detail whom the query can be directed to in your absence with contact details.
- Only use distribution groups such as SWC_AllStaff or SWC_AllStudents when justified for business needs.

- Use the Sensitivity labels identified in Oulook which is set by default to Public:
    - Internal Use
    - Restricted
    - Confidential
- If you do send an email incorrectly to anybody, this should be reported to your line manager, lecturer or directly to the Data Protection Officer or Information Security Officer for further guidance.
- Do not add, amend, or append anything to College email, which has not been approved or sanctioned by the College.
- Keep your personal emails relating to your employment in a separate folder from work related emails, such emails should be clearly marked ‘personal’ when being sent or received.
- If you are working outside of the UK or Ireland notify IT Services in advance in order that appropriate configuration settings can be applied for the required time.

2. Housekeeping

- Delete unnecessary emails.
- Clean your inbox regularly and delete old emails.
- Organise your messages into folders.
- Save important messages and attachments to your One Drive folder.
- When you exit your employment with SWC your email account will be closed so you must ensure that you have removed any personal emails that you may require for future use. You should also set an out of office notification redirecting the person to another member of staff.

3. Phishing

- You must complete all Phishing training required by the College and be alert to the following indicators of Phishing.
    - Email addresses that do not match the genuine organisation, visible by hovering your mouse over the email address.
    - Spelling mistakes in the email.
    - Generic greetings such as “dear valued customer.”
    - Requests for personal information.
    - Pressure to act quickly.
    - Congratulations on winning a prize.

- If in doubt, call the company or person with a contact number you have for them, not provided by the Phishing email, and confirm the information that is being requested by them is a genuine request.
- Report to IT Services for assistance in determining if the email is genuine.
- If an email has been quarantined, you will receive an email to inform you. You can access the quarantined email from the notification email and at your discretion either release the email for delivery or block and delete emails from that specific sender.

Appendix 2 – Guidance on the use of other College approved electronic communications platforms

1. Use of Social Media

1.1. The use of Social Media by staff is governed by the College's Social Media Policy and staff should familiarise themselves with this policy.

1.2. Social networking sites must only be used as a teaching and learning resource and the content must be professional, respectful, and responsible at all times.

1.3. If social networking sites are used in a personal capacity, care must be taken to ensure that your private interests and opinions do not damage the reputation of the College.

2. Microsoft Teams

2.1. Microsoft Teams is the approved platform for collaboration and communication. Teams is used as a more informal messaging method. However, staff must be circumspect in their use of Teams and follow guidance in relation to professionalism and respect as provided for email use. Teams communications are discoverable if searches are undertaken to respond to Access to Information requests and investigations.

3. All Other Electronic Communications Platforms

3.1. The guidance in relation to the use of Outlook and Teams applies to all College electronic communication platforms and they must be used professionally, respectfully, and not bring the College into disrepute.

Appendix 3 – WhatsApp

1. WhatsApp is not an approved communications tool and must not be used for College business on College or personal devices.

2. In limited and exceptional circumstances WhatsApp may be approved for external facing WhatsApp groups, external forums, and trips. Prior approval for the use of WhatsApp must be sought from the Director of Corporate Services or the Head of IT Services. Decisions will be based on the job role not the person, and at all times promotion of the use of Teams will be the first approach.

Related Documentation

Title	Location	Owner
Software Compliance Policy	Gateway	Director of Corporate Services
User Account Management Policy.	Gateway	Director of Corporate Services
Acceptable Use Policy	Gateway	Director of Corporate Services
Mobile Device Management Policy	Gateway	Director of Corporate Services
Data Protection Policy	Gateway	Risk & Compliance Officer
Clear Desk/Screen Policy	Gateway	Director of Corporate Services
IT Sec Security & Auditing Policy	Gateway	Director of Corporate Services
Hybrid Working Framework	Gateway	Head of People and Culture
Social Media Policy	Gateway	Marketing Manager

Change Log

Location	Change from deletion/addition	Change to
	New Policy	

Communication

Who needs to know (for action)	All Staff All Governing Body Members All Stakeholders All Visitors All Students
Who needs to be aware	As Above

Communication Plan

Action	By Whom	By When
Upload onto Gateway	Nicola Nugent	On approval and signing
Circulation to key staff	Director of Corporate Services	On approval and signing

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

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

Name	Organisation	Date
Management Operations Team	SWC	January 2024

Approval Dates

Approved by	Date
Governing Body	20 November 2024

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?
Internet and email usage policy V6.0	Nov 2023		Policy replaces with Electronic Communications Policy	N/A	Yes	Yes