IT08 Acceptable Use of IT Policy

Version Date: January 2025

Review Date: April 2028

NESCOL Acceptable Use of IT Policy

1. Policy Statement

1.1 The aim of this policy is to ensure that the IT Facilities at North East Scotland Colleges are used safely, lawfully and equitably and that individuals understand that they have personal responsibilities for ensuring information security and data protection.

1.2 This policy should be read in conjunction with, the Information Security Policy, Data Protection Policy, Social Media Policy and the IT Monitoring Policy.

2. Scope

2.1 This policy applies throughout the College, its IT infrastructure, its IT equipment (including mobile phones and devices) and its IT networks. It applies to all users of the College's IT on or off campus including staff, students and any third parties who use the College IT facilities.

2.2 The College IT facilities includes hardware, software, data, network access, third party services, online services or IT credentials provided or arranged by the College.

2.3 The IT facilities are provided to support the College's core business activities, primarily learning and teaching, plus all business functions to support these core activities.

3. Governance

3.1 When using the NESCol IT facilities, you remain subject to the same laws and regulations as in the physical world. When accessing services from another country, you must abide by all relevant local laws, as well as those applicable in the UK. Breach of any applicable law or third-party regulation will be regarded as a breach of this acceptable use policy (see Appendix 1).

3.2 You must abide by the regulations applicable to any other organisation whose network services you access. When using network services via the college IT facilities to any other organisation, you are subject to both the regulations of NESCOL and the organisation where you are accessing services. Some software licences procured by NESCOL will set out obligations for the user - these should be adhered to.

For more information on this please refer to section 6 of this policy.

3.3 Limited use of IT facilities for personal activities (provided it does not infringe on any other aspect of this policy and does not interfere with others' valid use) is permitted. If you use College email for personal purposes, personal emails should be marked with 'private' in the subject line and be moved to/stored in a mailbox folder labelled 'private'. Use of IT facilities for non-institutional commercial purposes, is not permitted.

All messages distributed through the College's e-mail system, even those of a personal nature can be subject to release if required by law.

4. Responsibility

4.1 IT Identity

4.1.1 You must not use the IT facilities unless you have been provided with IT login details (for example, a username and password, email address).

4.1.2 You must take all reasonable precautions to safeguard any IT login details issued to you.

4.1.3 You must not allow anyone else to use your IT login details. Nobody has the authority to ask you for your password and you must not disclose it to anyone.

4.1.4 You must not attempt to obtain or use anyone else's login details.

4.1.5 You must not impersonate someone else or otherwise disguise your identity when using the IT facilities.

4.2 Data/Information

4.2.1 All college data must be stored on the College provided Network Drives, VLE (MyNescol) or MIcrosoft365 productivity tools. Do not share, upload or post any college data, assessment or teaching materials (pre or post submission) via any 3rd party services e.g., 3rd party websites, social media platforms, email, cloud storage platforms etc.

4.2.2 If you have a requirement to work offline (e.g. whilst travelling) then OneDrive storage must be used. Data must not be stored to any physical device or storage (e.g. USB Drives) as this would increase the possibility of a data breach if the device is lost or stolen.

4.2.3 The College's supported method of sharing data with authorised external organisations is throughMicrosoft365 productivity tools. The college cannot guarantee the security of email services that it does not manage therefore personal email services (Hotmail, Gmail etc.) should not be used for college purposes e.g., the sending of college data between work and personal accounts, nor should personal accounts be used to distribute College data to 3rd parties.

4.2.4 You must not create, download, store or transmit unlawful material, or material that is indecent, offensive, threatening or discriminatory.

4.3 College data must not be stored on removable media (such as USB storage devices and removable hard drives,) or on personal mobile devices (laptop, tablet or smartphone). Security

4.3.1 You must not subvert or circumvent or attempt to subvert or circumvent College securitysafeguards such as firewalls, email filters or antivirus software.

4.3.2 You must not leave your computer unlocked when unattended - either lock it or log off.

4.3.3 When using the IT facilities, you must comply with all other relevant College policies and procedures.

4.3.4 You must not use unauthorised software, interfere with hardware or introduce malware tothe IT facilities.

4.3.5 All access to college systems locally and remotely must be via your college username/password, this includes the use of multi factor authentication (MFA).

4.3.6 You must not infringe copyright or break the terms of licences for software or other material.

4.3.7 Users are responsible for acting on any security instruction, guidance or advice or provided by the College.

4.4 Bring Your Own Device (BYOD)

4.4.1 NESCOL accepts the use of personal devices such as Smart Phones, Tablets, Laptops and PCs for work/course activity and this Acceptable Use Policy applies when these devices are logged in to or connected to the NESCOL network or systems.

4.4.2 Users are responsible for the maintenance of their devices including actioning software updates/patches and running antivirus software.

4.4.3 The users of personal devices should ensure there are adequate access controls enabled (password, PIN etc.).

4.4.4 No college data must be stored on personal devices (this includes all college related data and media).

4.4.5 For security purposes all user personal devices on campus are only allowed to securely connect to the College's campus network through Wi-Fi (NESCol or Eduroam). User personal devices must not be directly connected to the College's campus network via a physical wired connection.

4.4.6 The college will not routinely monitor personal devices. However, it does reserve the right to: prevent access to a particular device from connecting to college networks if unusual or illegal activity is detected. The college will also prevent access to a particular system and take all necessary and appropriate steps to retrieve information owned by the college if required.

4.5 Remote Working

4.5.1 When off campus it is the responsibility of the user to ensure the security of, college supplied devices particularly when working in public or unfamiliar settings. . It is advised that laptops and other devices should be carried as hand luggage when travelling.

4.5.2 You must not process sensitive information in public places (e.g., on public transport) where it might be viewed or heard by others.

4.5.3 Public WiFi hotspots (e.g., coffee shops and hotels) are not secure as there is no straightforward way to ascertain who controls or owns the hotspot. This can put your data at risk, so where possible opt for a trusted Wi-Fi connection, use a Virtual Private Network (VPN) or mobile 4G/5G network to ensure a secure connection.

4.5.4 Passwords for access to the College's systems must never be stored on personal or mobile devices where they may be stolen or permit unauthorised access to information assets.

4.5.5 Security risks (e.g., of damage, theft) may vary between locations and this should be considered when determining the most appropriate security measures. If you must work outside the UK as part of your role at NESCOL you must consider the access restrictions, data protection implications and other difficulties that you may encounter when using IT equipment in other countries.

4.5.6 To ensure you are given the most relevant advice relating to the country, users should contact the IT Helpdesk to discuss requirements in more detail prior to travel.

4.5.7 If a college device is lost or stolen or you have any security concerns please contact the IT Helpdesk immediately.

5. Monitoring

5.1 In order to ensure compliance with this policy, NESCOL monitors and records the overall use of its ITfacilities for the purposes of:

5.1.1 The effective and efficient planning and operation of the IT facilities.

5.1.2 Detection and prevention of infringement of these regulations.

5.1.3 Investigation of alleged misconduct.

5.2 Monitoring of individual use, and accessing data in individual user accounts, will only be undertaken by specific members of staff as a recognised part of their normal duties. Any such activity will be approved by the Assistant Principal - People Services and the relevant portfolio holder from the College Executive and be:

5.2.1 for legitimate business reasons; justifiable; fair; proportionate; not unnecessarily intrusive; and compliant with all applicable legislation including the UK General Data Protection Regulation, the Data Protection Act 2018 and the Human Rights Act 1998.

5.2.2 It is possible that personal data may be included in monitoring activity and may be inadvertently intercepted, reviewed and erased. For this reason, as well as for business continuity (see below), staff cannot be guaranteed complete privacy for permitted private use of email and internet facilities. Monitoring activity will be conducted in line with the NEScol IT Monitoring Policy.

5.3 NESCOL will comply with lawful requests for information from government and law enforcement agencies.

5.4 Authorised staff member access to an individual's email account may also be permitted when a member of staff is off work unexpectedly or for a prolonged period of time or has left College employment, so that nominated authorised staff members may obtain business related documents or correspondence to ensure business continuity, or so that information required for subject access/freedom of information requests can be retrieved. Such access will be permitted and carried out in line with the Email Access Procedure, ensuring that:

5.4.1 Only data, including personal data, that is needed to carry out a defined task is accessed and processed

5.4.2 Every effort is made to avoid accessing content which can be identified as personal

5.4.3 Access is undertaken by specific members of staff and is approved in advance by the Assistant Principal - People Services.

6. Compliance

6.1 Infringing this Policy may result in sanctions under NESCOL's Disciplinary Policy and Procedure. For staff this would be dealt with through the disciplinary procedure and for students this would be through the student disciplinary policy and procedures.

6.2 If the disciplinary process finds that you have breached this policy, sanctions may be imposed

6.3 For contractors or third-party organisations, breach of this policy will lead to remedies for NESCOL as detailed within the relevant contract.

6.4 Information about infringement may be passed to appropriate law enforcement agencies, and anyother organisations whose regulations you have breached. You must abide by the law when accessing NESCOL's IT facilities.

6.5 If you become aware of any infringement of this policy, you must raise a call with the IT Helpdesk.

7. Review

7.1 This policy will be reviewed every three years or as required.

Status:	Final	**Summary of changes**
Approved by:	Executive Team	Changes to reflect new job titles. Minor wording changes to improve and clarify the understanding of policy. Para 4.4.6 removed – not relevant
Date of version:	January 2025	
Date of Consultation:	November 2022 (EIS & UNISON)	
Responsibility for Policy:	Assistant Principal - IT & Digital Services	
Responsibility for Review:	Information Security & Data Protection Manager	
Review date:	April 2028	
DPIA date:	January 2025	
EIA date:	January 2025	

DATA PROTECTION IMPACT ASSESSMENT (DPIA)

1. **Does the activity that this policy or procedure relates to use personal data in any way?** (Use may refer to collecting and gathering; storing electronically; storing by paper; sharing with other parties (internal or external to college); use of images as well as written information; retaining and archiving; or erasing, deleting and destroying)	Yes
2. **Does the activity that this policy or procedure relates to use special category personal data in any way?** (Special category data is data about: race; ethnic origin; politics; religion; trade union membership; genetics; biometrics (where used for ID purposes); health; sex life; or sexual orientation)	Yes
3. **Does the activity that this policy or procedure relates to involve the use of social media or a third-party system?**	YES – MS365

If the answer is 'yes' to one or more of the above questions, the Data Protection Officer must be consulted.

Date of DPO consultation:	January 2025
Description of outcome and actions required (if any): DPO has been involved in the development of this policy. All DP considerations and requirements have been incorporated. DPIA completed as part of use of associated systems such as VLE, MS 365 etc	
DPIA screening/full DPIA required:	No

EQUALITY IMPACT ASSESSEMENT (EIA)

Part 1. Background Information

Title of Policy:	NESCol IT Acceptable Use Policy
Person Responsible:	Malcolm Johnson
Date of Assessment:	January 2025
What are the aims of the Policy?	This policy sets out the colleges expectations for acceptable use of ICT systems and services.
Who will this Policy impact upon?	All staff and students.

Part 2. Public Sector Equality Duty Comparison
(Consider the proposed action against each element of the PSED and describe potential impact, which may be positive, neutral or negative. Provide details of evidence.)

Need	Impact	Evidence
Eliminating unlawful discrimination, harassment and victimisation	Positive	This policy is to ensure that the IT Facilities at North East Scotland Colleges are used safely, lawfully and equitably and that individuals understand that they have personal responsibilities for ensuring information security and data protection.
Advancing Equality of Opportunity	Positive	As above
Promoting good relations	Positive	As above

Part 3. Action & Outcome (Following initial assessment, describe any action that will be taken to address impact detected)

No action is required.

Sign-off *	
Name:	Malcolm Johnson
Position:	Information Security & Data Protection Manager
Date of original EIA:	January 2017
Date EIA last reviewed:	January 2025

**Please note that an electronic sign-off is sufficient*

Appendix 1:

- Computer Misuse Act 1990 - creates offences of unauthorised access and interference withcomputers and data.
- Communications Act 2003 - creates offences of improper use of a public communications service(s.127) and dishonestly obtaining electronic communications services (s.125).
- Investigatory Powers Act 2016 - controls the interception of traffic on networks. It also creates powers for the police and other investigating authorities to require networks to provide informationabout their users and their use of networks.
- The Investigatory Powers (Interception by Businesses etc. for Monitoring and Record-KeepingPurposes) Regulations 2018 - covers interception for business purposes, for example the enforcement of acceptable use policies.
- Data Protection Act 2018 and UK General Data Protection Regulation - establish requirements on anyoneholding personal data on a computer or any other organised filing system.
- Privacy and Electronic Communications (EC Directive) Regulations 2003 - contains detailedrestrictions on the use of personal data in electronic communications (for example sending unsolicited e-mails), amended by the Privacy and Electronic Communications(EC Directive)(Amendment) Regulations 2011.
- Freedom of Information (Scotland) Act 2002 – gives a legislative right for anyone to ask for any information held by a Scottish public authority.
- Defamation Act 1996 and Defamation Act 2013 – protects individuals and organisations from slander and libel when untrue, damaging information about someone is published to a third party.
- Counter Terrorism and Security Act 2015 – makes provisions in relation to terrorism, including provisions about the retention of communications data
- Police and Criminal Evidence Act 1984 – covers powers and duties of the police, including in relation to seizing of information as criminal evidence.
- Copyright, Designs and Patents Act 1988 – lays out a framework of rules on how work can be used, setting out the rights of owners as well as responsibilities of other people who want to use the work.