ICT Acceptable Use Policy for Non-College User

Overall responsibility: Julian Wood	Deputy Principal (Finance & Corporate Affairs)
Implementation: Ashok Dave	Department: ICT Services
Date issued:	March 2024
Date for review:	March 2025

Endorsed and approved by Policy & Strategy Group Date: 12.3.24

Pat Brennan-Barrett Principal

Contents

1. INTRODUCTION

Users are expected to use all ICT equipment, Internet access and college data primarily for college business and education related purposes. Users who are not staff or students at the college are considered as a non-college user. As a non-college user, you are expected to conduct yourself honestly and appropriately when using ICT resources including data and the Internet, and respect the copyrights, software licensing rules, property rights, privacy and prerogatives of others. All existing college policies apply to the use by, and conduct of, visitors using ICT resources, data and the Internet, especially (but not exclusively) those policies that deal with intellectual property protection, privacy, misuse of college resources, safeguarding, sexual harassment, information and data security, general data protection regulation and confidentiality.

2. RESPONSIBILITY

Deputy Principal – Finance and Corporate Affairs

3. SCOPE

ICT equipment and associated technologies are used to support learning, the college business and to enhance knowledge. Computer Networks allow access to the Internet, email, personal and shared folders, and allow people to interact with other computers and networks and with a multitude of electronic users.

The deployment and use of the College's ICT systems; all computers, peripheral equipment, software and data within and between Northampton College property, or belonging to the college but located elsewhere.

It includes connection to external systems by college equipment and all use of the college's computer networks, email facility, website(s), intranet, internet and cloud use.

The security of hardware, software and data, the security of personnel using ICT systems, and the security of the college's assets that may be placed at risk by misuse of ICT systems.

In respect of copyright and data protection aspects, the policy covers the use of ICT systems not only owned by the college or located on its property but also used by college students or staff for study or business purposes connected with the college.

4. POLICY STATEMENT

This policy is designed to help visitors, contractors, associates and non-employed educational and other user's, understand college wide expectations for the use of ICT resources, and sets out clear guidelines which must be adhered to. These users will be honorary members of staff with restricted facilities.

It is expected that as a general policy, all ICT equipment and computer networks will be used in a responsible, efficient, ethical and legal manner.

This policy is designed to help visitors understand college wide expectations for the use of these resources and sets out clear guidelines which must be adhered to.

5. KEY PRINCIPLES

- All non-college user will be required to read and sign an ICT Acceptable Use Policy for Non-College Staff form before being issued with a temporary computer account.
- This form will detail activities that are acceptable and not acceptable and additional general guidance information.
- Refusal to sign the form will result in denial of access to college systems.
- The College has software and systems in place that can monitor and record all Internet usage and emails. The security systems are capable of recording (for each and every user) each web site visit, chat, newsgroup, e-mail message, and each file transfer into and out of the college's internal networks and cloud services.
- The College reserves the right to use these systems where appropriate to monitor correct network, Internet and e-mail usage**.**

6. THE PROCEDURE

A) UNACCEPTABLE USES OF ICT SERVICES

The following activities are examples of unacceptable uses of ICT Services:

- Using the Internet for any illegal purpose.
- Using the network/Internet for any activity promoting terrorism or radicalisation or any activity covered by the Counter Terrorism and Security Act (Prevent Act).
- Storing, sending or knowingly receiving any information that includes pornography, unethical or illegal solicitation, inappropriate language, and/or information used to promote racism or sexism. Sexually explicit material may not be displayed, archived, stored, distributed, edited or recorded using the College network or computing resources.
- Sending or knowingly receiving, storing or using copyrighted materials, videos and music without the owner's permission.
- Distributing software or materials in violation of the General Data Protection Regulation or distribution licence.
- Installing or downloading illegal, pirated or unlicensed software.
- Using the network/Internet to deliberately propagate any virus, worm, Trojan horse, or malicious code.
- Using the network/Internet for financial gain or commercial activity.
- Violating any person's right to privacy.
- Using the network/Internet for product advertisement or political lobbying.
- Changing/deleting files which do not belong to the user.
- Using the network/Internet to make unauthorised entry into other computational, informational or communication services or resources (Hacking).
- Using another person's username and password or allowing someone else to use their password, without prior authorisation from one of the ICT Managers.
- Storage of non-college related data such as personal photos, music etc.
- Installing or connecting unauthorised equipment to the college network for illegal purpose.
- Inappropriate use of your college identity on social networking sites.
- Physical damage to any ICT equipment or services
- Removal or relocation of any ICT equipment without appropriate permission.
- Copying staff or student's personal data and taking off site unless in an encrypted format or accessing such data from an external source including approved cloud storage (See Data Protection policy and ICT Security Policy).
- Bypassing the firewall using a proxy service.
- Accessing any college data without authorisation.
- Using data for any purpose other than that it was supplied for.

- Using remote access software except college supplied software in classrooms for educational use.

B) RESPONSIBILITY OF A USER

A responsible education user will:

- Be polite and never send or encourage others to send abusive messages.
- Use appropriate language and promote high standards in 'Netiquette'.
- Delete old messages and stored files on a regular basis. (Housekeeping of emails and files is very important so that the data storage areas are not clogged up with unwanted files and emails).
- Comply with the General Data Protection Regulation and Copyright legislation.
- Comply with the ICT Security Policy.
- Comply with BYOD Policy.
- Treat all ICT equipment with respect and keep it always secure.

C) THINGS TO CONSIDER

- Non-College User may use their Internet facilities for non-business research or browsing during breaks, or outside of work hours, provided that all usage policies are adhered to. The college management reserves a right to charge for the use of Internet and Email for personal use.
- Non-College Staff with Internet access may not use college Internet facilities to download and/or store music, entertainment software or games, or to play games against opponents over the Internet.
- User with Internet access may not upload any software licensed to the college or data owned or licensed by the College without explicit authorisation from the Head of ICT Services or his deputy.
- Any software or files downloaded via the Internet into the college network will become the property of the college. Any such files or software may be used only in ways that are consistent with their licenses or copyrights. The college reserves the right to inspect any files stored in private areas of the college network or on the college computers to assure compliance with college policy.
- The college has software and systems in place that can monitor and record all network, Internet usage, emails, and cloud storage. The college reserves the right to use these systems where appropriate to monitor correct Internet and e-mail usage and for the purposes of the PREVENT strategy.
- Ensuring any data accessed from non-college equipment both internally and externally is secured appropriately and not shared with any third party.

D) PASSWORD RECOMMENDATIONS

- Staff user account must use a complex password, it must be a minimum of 12 characters and contain at least 3 of the following 4 requirements: 1) An Uppercase Letter, 2) A Lowercase Letter, 3) A Number, 4) A Special Character (for example @, !, $, etc). NCSC (National Cyber Security Centre) suggests using three random words in mixed case separated with punctuation.
- Don't use a password that is the same or like one you use anywhere else.
- Make passwords hard to guess, even by those who know a lot about you, such as the names and birthdays of your friends and family, your favourite bands, and phrases you like to use.
- Do not reuse organisation password anywhere else. The use of organisation passwords in external websites greatly increases the likelihood that cybercriminals will compromise these passwords.
- If a password is suspected to be compromised, it should be changed immediately.
- Usernames, staff numbers, and passwords should be protected appropriately. If a password manager is used, the master password should be stored securely.

E) ARTIFICIAL INTELLIGENCE

The use of Artificial Intelligence (AI) in the college is guided by principles of ethical use, data privacy, and academic integrity. We are committed to using AI responsibly, ensuring it is used for educational enhancement, and not for plagiarism or other unethical activities. We regularly review our AI usage and stay updated with the latest developments in AI technology to ensure our practices are current and in line with legal and ethical standards.

7. REPORTING

Any breach of the ICT Acceptable Use Policy should be reported to the Head of ICT services or Deputy Principal – Finance and Corporate Affairs. Where such action is outside of the remit of ICT Services, the Deputy Principal (Finance & Corporate Affairs), the Head of ICT Services will notify the appropriate officer(s) of the College or appropriate authorities.

8. ASSOCIATED POLICIES

- BYOD Policy
- ICT Security Policy
- Data Protection Policy
- Staff Disciplinary Policy
- Safeguarding.

9. APPROVAL PROCESS

- Policy and Strategy

10. APPENDICES:

Appendix 1: Diversity Impact Assessment

Appendix 2: Data Protection

Appendix 3: Communication

Appendix 1: EQUALITY & DIVERSITY IMPACT ASSESSMENT

This template has been designed to help you take action to improve services and practices which affect staff, students and other service users at Northampton College. By completing this template, you would have considered the impact that your policy, practice or service might have on particular social groups within the college community. The exercise will also provide you with the opportunity to demonstrate, where possible, that the College promotes equity, diversity and inclusion.

Once this Equality Impact Assessment has been created, please include on the last page of your policy document.

Policy Details	
What is the policy?	ICT Acceptable Use Policy for Non-College user
Is it new or existing?	Existing
Department	ICT Services
Policy Author (postholder title, name)	Ashok Dave – Head of ICT Services
Author of Equality Analysis	
Date of completion	05/03/2024

Aim and Objectives
Briefly describe the aims and objectives of the policy
To ensure that visitors to the college using college systems understand their obligations when using college systems. To ensure college complies with its legal and Janet requirements.

Policy Assessment				
Consider whether your policy might have an impact on various groups identified within the categories listed below and explain why you have reached this conclusion. Please tick (√) the identified level of impact (positive, negative, or no impact) and provide details of your findings.				
	Positive Impact	Negative Impact	No Impact	Findings
Race			x	
Religion and/or belief			x	
Sex (Gender)			x	
Gender Identity			x	
Disability			x	
Age			x	
Sexual orientation			x	
Marriage and/or civil partnership			x	
Pregnancy and/or maternity (including surrogacy and adoption)			x	
Other identified group (e.g. carers)			x	

Action Planning		
How do you intend to mitigate or eliminate any negative impact identified?	If a positive impact is identified, how do you intend to promote or develop this opportunity?	Where negative impact has been identified, can it be justified? If so, explain how.

Monitor and Review		
How will you monitor the impact of your policy once it has been put into effect?		
The policy will be monitored through feedback from services users gathered via: Policy and Strategy		
Names and position of Impact Assessment Team (min of 3 preferably from areas across the College):		
Name		
Mark Owen	Assistant Principal – Student Services	
Bob York	Deputy Director of Estates	
Ashok Dave	Head of ICT Services	
Equality Analysis Sign-Off Signature and Date:		05/03/2024
Review Date:		05/03/2025

Appendix 2: DATA PROTECTION IMPACT ASSESSMENT

Data Protection Impact Assessment

Does this Policy

- require the collection and use of data in addition that normally collected by the College?

Yes / No (if Yes complete Assessment point number 1)

- require the sharing of data with partners?

Yes / No (if Yes complete Assessment point number 2)

1. Is additional data being collected? If so please detail:

No

Is data collected personal and/or sensitive?

Yes

How will you collect, use, store and delete data?

The data is stored on system logs which are periodically deleted. These logs are only available through admin privileges and are audited.

2. Will you be sharing data with anyone? Please detail what data, with who and confirm a **Data Sharing Agreement** is in place

No

Describe the purposes of the processing / sharing: What are the benefits of the processing/ sharing – for you, and more broadly?

This is a requirement by JANET part of their acceptable use policy and is a legal requirement.

Consider how to consult with relevant stakeholders: describe when and how you will seek individuals' views – or justify why it's not appropriate to do so.

User must read, sign and agree to the policy before access is granted.

Describe compliance and proportionality measures, in particular:
What is your lawful basis for processing?

Required by Janet our network provider and by law.

How will you ensure data quality and data minimisation?

Only data collected by the systems are stored. This is overwritten/delete periodically.

What information will you give individuals?

None

Please attach a Risk Assessment if there are significant risks to data protection.

Signed by Data Protection Officer

Name: Julian Woods

Date: 5th March 2024

Appendix 3: COMMUNICATIONS PLAN

TITLE OF COLLEGE POLICY:	DATE APPROVED BY
ICT Acceptable Use Policy for Non-College User	Date: 12/03/2024

AUDIENCE (select appropriate with √)					
Managers		Curriculum teams		Business Support teams	
All staff		Suppliers		Partners	x
Other - Students					

CHANNEL (select appropriate with √)					
Policy & Strategy Team (PST)	x	Quality Improvement Network (QIN)		Marketing team	
Meeting		Meeting		NC Update Intranet Website	x
Individual team		Suppliers		Partners	
Document Library Noticeboards Team meeting Email		e.g. Letter or email Meeting		e.g. Letter or email Meeting	
College Management Team (CMT)		JCNC		CORPORATION	
Meeting		e.g. Meeting Email		e.g. Meeting Email	

COMMUNICATIONS PLAN ACTIVATED BY:		
Name: Ashok Dave Department ICT Services	Job title: Head of ICT Services	Date: 12/03/2024

Appendix 4: USER ACCEPTANCE FORM

Acknowledgment

I acknowledge that I have received this written copy of the Information Communications Technology Acceptable Use Policy for Non-College User' of Northampton College. I understand the terms of this policy and agree to abide by them. I realise that the College's security software may record and store for management use the electronic e-mail messages I send and receive, the Internet address of any site that I visit, and any network activity in which I transmit or receive any kind of file. I understand that any violation of this policy could lead to action being taken and possible criminal prosecution.

Signature …… Name …….

(Capitals)

Date …. …… Date of Birth ……..……..

DOB Needed to generate initial password

College Contact……. Reason for Application…….
(Capitals)

This policy has been checked under the Equality and Diversity guidelines and found not to cause disadvantage to any specific groups. Should this policy be required in any other format, this can be arranged by ICT Services who will liaise with the Additional Support team.