

POLICY STATEMENT

TITLE:

ICT Acceptable Usage Policy for Non-College Staff

INTRODUCTION/OVERVIEW:

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.

POLICY STATEMENT:

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 users understand college wide expectations for the use of these resources, and sets out clear guidelines which must be adhered to.
Failure to adhere to these guidelines could result in action being taken.

QUALITY STATEMENTS:

- Everyone will be required to read and sign an ICT Acceptable Usage Policy form before being issued with a computer account and an email address.
- 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 a computer account.
- Action will be taken against anyone not complying with the policy by removing their network privileges and may be reported to appropriate authorities.
- 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 World Wide Web site visit, each chat, newsgroup or e-mail message, and each file transfer into and out of the College's internal networks.
- The College reserves the right to use these systems where appropriate to monitor correct network, Internet and e-mail usage.

**LINKED POLICIES/
PROCEDURES:**

- ICT Security Policy
- Data Protection Policy
- Prevent Strategy 2011
- Safeguarding

MONITORING PROCEDURE:

- Executive Director of Estates
- Head of ICT Services
- ICT Services Managers
- Periodic Review


**DATE FOR REVIEW AND NEXT
DIVERSITY IMPACT
ASSESSMENT:**

September 2019

RESPONSIBILITY:
Overall (Directorate/Dept):
Implementation:

Executive Director of Estates

APPROVED BY SMT:
(Principal to sign)

 (Signature)

Pat Brennan-Barrett (Position)

19/9/18 (Date)

OR

**ENDORSED BY SMT AND
APPROVED BY CORPORATION:**
(Principal to sign)

(Signature)

Pat Brennan-Barrett (Position)

(Date)

ICT Acceptable Usage Policy for Non-College Staff

Scope of Policy

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. 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. Failure to adhere to these guidelines could result in action being taken.

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

Overview

You are expected to use all ICT equipment and Internet access primarily for college business and education related purposes. As a non-college member of staff you are expected to conduct yourself honestly and appropriately when using ICT resources 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 honorary staff using ICT resources and the Internet, especially (but not exclusively) those policies that deal with intellectual property protection, privacy, misuse of College resources, safeguarding, sexual harassment, General Data Protection Regulation, information and data security, the PREVENT agenda and confidentiality. Unlawful Internet usage and sharing/loss of college data may also attract negative publicity for the College and expose the institution to significant difficulties.

The following activities are 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 PREVENT strategy 2011.
- 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.
- 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 and/or data 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 (See Data Protection policy and ICT Security Policy).
- Bypassing the firewall using a proxy service.

A responsible 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.
- Treat all ICT equipment and data with respect and keep it secure at all times.

Other things to consider

- Non-College Staff 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.
- Non-College Staff 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 in order to assure compliance with college policy.
- The College has software and systems in place that can monitor and record all network, Internet usage and emails. 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 2011.
- Ensuring any data accessed from non-college equipment both internally and externally is secured appropriately and not shared with any third party.

Acknowledgment

I acknowledge that I have received this written copy of the Information Communications Technology Acceptable Use Policy for Non-College Staff' 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
(Capitals)

Date of Birth
(Capitals) **DOB Needed to generate initial password**

College Contact.....
(Capitals)

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.

Appendix A

EQUALITY & DIVERSITY IMPACT ASSESSMENT

This form should be used by managers and policy authors within their area of responsibility to carry out Equality & Diversity Impact Assessments (E&DIAs) in relation to protected characteristics, specifically: Age, Sex, Disability, Gender reassignment, Race, Religion or Belief, Sexual Orientation, Pregnancy & Maternity and Marriage & Civil Partnership.

The word 'policy' is taken to include strategies, policies, procedures and guidance notes; formal and informal, internal and external.

The Impact Assessment may be carried out on any policy, service, function or plan you are engaged in, or are about to commence. All policies should be clearly stated. However, in reality, some policies are built into everyday procedures and customs, therefore not all policies are open to inspection and review. Any assessment of a policy should include these customs and practices as well as the formal written policy. 'Functions' means your duties and powers and includes internal and external functions, including service delivery.

1. Name of policy

ICT Acceptable Usage Policy for Non-College Staff

2. What is the aim(s), objective(s) and/or purpose of the policy?

To ensure that visitors of the college using college systems understand their obligations when using college systems. To ensure college complies with its legal and Janet requirements.

3. Who is the policy lead?

Ashok Dave – Head of ICT Services

4. Which of the following groups could be affected by this policy? (Tick all that apply)

Learners

Staff

Wider community ✓

5. Team

Names and position of Impact Assessment Team (min of 3 preferably from areas across the College):

Name	Position
Ashok Dave	Head of ICT Services
Bob York	Deputy Director of Estates
Phil O'Hara	Head of school -STEM

Date E&DIA undertaken: ___14/09/2019_____

E&DIA undertaken as a result of:

Renewal / Revision of Policy / Procedure

New Policy / Procedure

SAR process

Other Please state _____

Date of last E&DIA (if applicable) 09/08/2017

6. Complaints?

Have complaints been received from anyone with one or more protected characteristic about the service provided? If yes then please give details.

No Yes

--

7. The Impact

Four possible impacts should be considered as part of the assessment:

- Positive impact** – Where the policy might have a positive impact on a particular protected characteristic.
- None or little impact** – Where you think a policy does not disadvantage any of the protected characteristics.
- Some impact** – Where a policy might disadvantage any of the protected characteristics groups to some extent. This disadvantage may be also differential in the sense that where the negative impact on one particular group of individuals with protected characteristics is likely to be greater than on another.
- Substantial impact** – Where you think that the policy could have a negative impact on any or all of the protected characteristics. This disadvantage may be also differential in the sense that the negative impact on one particular protected characteristic is likely to be greater than on another.

Using the guidance provided above, complete the following table:

Sex/Age	Positive impact	No or little impact	Some adverse impact	Substantial adverse impact
Women		✓		
Men		✓		
Age		✓		

Disability	Positive impact	No or little impact	Some adverse impact	Substantial adverse impact
Visually impaired		✓		
Hearing impaired		✓		
Physical disability		✓		
Specific Learning difficulties		✓		

Global learning difficulties		✓		
Autistic Spectrum Disorder		✓		
Any other disability - various		✓		

Race	Positive impact	No or little impact	Some adverse impact	Substantial adverse impact
White		✓		
Other minority groups		✓		

Other Protected Characteristics	Positive impact	No or little impact	Some adverse impact	Substantial adverse impact
Religion and Belief		✓		
Sexual Orientation		✓		
Gender Reassignment		✓		
Pregnancy & Maternity		✓		
Marriage & Civil Partnership		✓		

Please comment on any areas where some or substantial impact is indicated. Any resulting actions must be added to the attached action plan.

8. Is there anything that cannot be changed? No

What cannot be changed?	Can this be justified?	If so, how?

Please list the main actions that you plan to take as a result of this assessment in your area of responsibility. (Continue on separate sheets as necessary)

DISTRIBUTION: Copies of the final E&DIA should be sent to:

- Jan Hutt - Director of HR
- Patrick Leavey - Deputy Principal – Teaching, Learning & Success
- Quality Improvement Team Administrator

And to those whom this Impact Assessment will cause to have further work to do in either changing processes or re-writing the policy(s) concerned.

All actions recorded here should be carried forward into your QIP, so that actions can be monitored and evaluated to measure the impact. There will be random sampling of action plans through the Equality & Diversity Forum.

APPENDIX B

COMMUNICATIONS PLAN

TITLE OF COLLEGE POLICY: ICT Acceptable Use Policy for Non-college staff	DATE APPROVED BY Policy & Strategy Group Or Corporation Date:
--	--

AUDIENCE (select appropriate with √)			
Managers		Curriculum teams	Business Support teams
All staff		Suppliers	
Other (please state)		Visitors	√

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

COMMUNICATIONS PLAN ACTIVATED BY:		
Name: Gary Brough	Job title: Executive Director of Estates	Date: