ICT Security Policy

Overall responsibility: Julian Wood	Deputy Principal Finance and Corporate Affairs
Implementation: Ashok Dave	Department ICT Services
Date issued: 1st September 2024	
Date for review: 1st September 2025	

Endorsed and approved by Policy & Strategy Group September 2024

Jason Lancaster Principal

Contents

1. INTRODUCTION

ICT Systems at college are used to support learning and to enhance knowledge.

Computer Networks and ICT Systems can be damaged by misuse, vandalism, hacking, virus attacks and several other means, both locally and via the Internet.

This policy details the responsibilities of staff when using college systems.

2. RESPONSIBILITY

Deputy Principal – Finance and Corporate Affairs.

3. SCOPE

The Policy covers:

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 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

Northampton College seeks to protect its ICT assets and data from loss and to provide a secure working environment for its students and staff. The objectives of the Policy are to ensure as far as is reasonably possible that:

The College's assets are secure against loss by theft, fraud, malicious or accidental damage, or breach of privacy or confidence, and The College is protected from damage or liability resulting from use of its facilities for purposes contrary to the law of the land or the College's Charter.

5. KEY PRINCIPLES

Ensure robust security is in place for ICT equipment and systems. It is the specific responsibility of the Deputy Principal of Finance and Corporate Affairs to ensure that the Policy is carried out. All students, staff and visitors have a personal responsibility to ensure that they, and others who may be responsible to them, are aware of and comply with the Policy.

6. THE PROCEDURE

A) ACCEPTABLE USE

All users must read, accept the terms, and sign the appropriate Acceptable Use Policy before being allowed to have a logon and password to the College systems.

Acceptable use is defined as use for the purposes of:

- Teaching and learning
- Research
- Personal educational development
- Administration and management of college business
- Development work and communication associated with the above
- Consultancy work while contracted to the college.
- Reasonable use of computer facilities for personal correspondence, where not connected with any commercial activity, is at present regarded as acceptable at the discretion of the person's manager or tutor.
- Use for other purposes may be permitted by the Vice Principal (Resources) or the Head of ICT Services.

Detailed lists of acceptable (and non-acceptable) use are available in the Staff, Non-employed User's and Student Acceptable Use Policies (AUPs).

Users of the Internet will also need to comply with the JANET Acceptable Use Policy and the Janet Security Policy.

It is College policy that there will be a Code of Good Conduct which will be reviewed regularly and circulated to all members of the College. All users are expected to abide by the Code.

It is College policy that all use of the facilities shall be lawful, honest and decent, and shall have regard to the rights and sensitivities of other people.

The Deputy Principal (Finance and Corporate Affairs), together with the Head of ICT Services and ICT Services Managers has responsibility to take all reasonable steps to stop unacceptable use of ICT systems. These officers will be guided on policy issues by the College Executive Team and advice from appropriate external bodies.

B) REGISTERED USERS

The following are eligible to register as users and must complete the appropriate AUP if seeking to use ICT in scope of this policy:

- Any student currently registered on a course.
- Any person currently holding a contract of employment with the College.
- Any person appointed as a Governor to the College.
- Any person holding an honorary position recognised by the College.
- Any person acting as a contractor/advisor to the College.
- Any person of another educational establishment, teaching on the premises.
- Any person authorised by the Deputy Principal (Finance & Corporate Affairs), Head of ICT Services or ICT Services Managers.

Specific data systems may require additional log on facilities for these users.

Approval for all systems is not automatic and is at the discretion of the Deputy Principal (Finance & Corporate Affairs), Head of ICT Services, ICT Services Managers.

Apart from access to material intended for the public, use of information systems and networks shall be restricted to registered users. The Deputy Principal (Finance & Corporate Affairs), Head of ICT Services, ICT Services Managers, as appropriate, has responsibility for implementing such access restrictions.

Temporary public wireless access that only allows connection to the Internet for guests and visitors may be granted. Wi-Fi access can be requested through ICT Helpdesk. Access may be granted subject to the user agreeing to college's acceptable use policy.

C) OPERATIONAL PRACTICE

It is the responsibility of the Deputy Principal (Finance & Corporate Affairs), Head of ICT Services and ICT Operations Manager to attend to the following:

- Securing the integrity of data and software held and processed on the College's information systems.
- Securing the integrity of data stored in cloud.
- Robust backup and restoration facilities of all central systems.
- Securing the integrity of all data storage areas, cloud storage, servers & computers.
- Ensuring file stores of servers & computers are secure and purged of inappropriate material, especially copyrighted material.
- In the event of a suspected security breach, enforcing appropriate restrictions to the service and user account until confidence is restored.
- Provision of appropriate antivirus, anti-spyware, anti-spam, anti-phishing, anti-malware, other security and protection tools on computer equipment under their control.
- Provision of effective controls on access to restricted facilities, such as business support data systems, cloud storage and shared storage areas.
- Provision of an appropriate software update system for servers and computers.
- Provision of a central firewall blocking facility for web access allowing the college to restrict inappropriate use and specific facilities and websites.
- Provision of blocking inappropriate and potential security risk emails through appropriate monitoring systems.
- Provision of an encryption system to restrict access to data taken offsite.
- Provision of advice and guidance on Information and Data Security matters.
- Provision of a remote access system for approved use only.
- Any other security measures that may become necessary at any time.

It is the responsibility of the computer user to attend to the following:

- Taking appropriate security precautions in respect of computers under their control.
- Observing good practice recommendations for security in respect of facilities provided on computers and networks.
- Keeping their username and password secret.
- Using the appropriate encryption technique when sending data in external emails.
- Using the appropriate encryption technique when it is necessary to take data off site on laptops, USB drives and other portable disks or devices.
- Reporting breaches of security to the ICT Services Team.
- Not connecting inappropriate equipment to the network.
- Only using college installed remote access software and in an approved manner.

- Use of college approved cloud storage such as One drive for Business to store college related data.
- Damage to equipment, software or data resulting from failure to observe this policy is deemed to be the responsibility of the defaulter.
- College data should not be emailed/forwarded/saved to personal accounts.

Control of access to personal data is the remit of the College's Data Protection Officer, who will ensure that information about rights and responsibilities under the General Data Protection Regulation is made available.

D) 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.

E) PHYSICAL SECURITY

All college equipment will be secured against theft and damage to a level that is cost-effective.

Users must not physically connect unauthorised non-college equipment to the network.

Equipment loaned to staff must be kept in a secure environment when not in immediate use and they may be held responsible for any losses if considered irresponsible.

F) MONITORING/LOGGING

The Deputy Principal (Finance and Corporate Affairs), Head of ICT Services or ICT Services Managers, as appropriate, are responsible for ensuring that usage of resources will be logged in sufficient detail and at an appropriate level to identify defaulters where technically possible.

The Deputy Principal (Finance & Corporate Affairs), Head of ICT Services, as appropriate, will authorise ICT Services staff whose duties require them to monitor and police the use of computer facilities. Monitoring data will be collected only to assist investigation of a suspected security breach or other misuse, including activities covered by the PREVENT Strategy

ICT Services staff shall not monitor personal information except in specific instances where a suspected breach of security or other substantive offence requires it. Every such incident will be centrally recorded, and serious incidents will be reported to the Deputy Principal (Finance & Corporate Affairs), the Head of ICT Services and the data protection officer. The central record will be made available for inspection by personnel authorised by the principal.

The Deputy Principal (Finance & Corporate Affairs), the Head of ICT Services, as appropriate, are empowered to authorise a hardware and/or software audit of college equipment, where it is deemed necessary and to authorise removal of offending items.

The college may use services such as Dark Web monitoring to protect the college and its users.

G) ICT SECURITY ADVICE AND TRAINING

It is the responsibility of the Deputy Principal (Finance & Corporate Affairs) to ensure that all users are made aware of the risks of security breaches and of their responsibility to take adequate precautions.

The Head of ICT Services, ICT Services Manager or other nominated senior ICT Services staff will undertake this by:

- Giving appropriate security information during staff inductions.
- Publishing articles in NC Update and Managers Update.
- Publishing advice on the staff Intranet.
- Email reminders.
- Any other method as deemed appropriate.

H) DUTIES OF ICT SERVICES STAFF

ICT Services Staff have responsibility for maintaining the integrity of computer systems and data held on them, ensuring appropriate backups and for ensuring the systems are not misused.

ICT Services Staff are provided with privileged access to computer systems to carry out their responsibilities. They have a specific duty to always use such privilege in a professional manner and within the interest of the College. Abuse of this privilege will result in disciplinary action and/or dismissal.

Deputy Principal (Finance & Corporate Affairs), together with the Head of ICT Services and ICT Services Managers, as appropriate, are responsible for ensuring that the duties of ICT Services staff are carried out correctly and will publish and maintain details of ICT Services Staff and the domain of their responsibilities.

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

7. REPORTING

BREACH REPORTING:

It is the duty of the Deputy Principal (Finance & Corporate Affairs), together with the Head of ICT Services and ICT Services Managers to take appropriate action to prevent breaches of the policy. Where such action is outside of the remit of ICT Services, the Deputy Principal (Finance & Corporate Affairs) or the Head of ICT Services will notify the appropriate officer(s) of the College or appropriate authorities. All breaches should be reported to Head of ICT services or ICT Services manager.

8. ASSOCIATED POLICIES

The Policy is to be read in the context of the following legislation:

The General Data Protection Regulation (GDPR)

Copyright, Designs and Patents Act

Computer Misuse Act

Criminal Justice and Public Order Act

Freedom of Information Act

Regulation of Investigatory Powers Act.

And any other relevant legislation, current or future.

9. APPROVAL PROCESS

- Policy and Strategy.

10. APPENDICES:

Appendix 1: Equality and Diversity Impact Statement

Appendix 2: Data Protection Impact Statement

Appendix 3: Communication Strategy

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 Security Policy
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	18/09/2024

Aim and Objectives
Briefly describe the aims and objectives of the policy
To ensure the college systems are secure and staff, students, and visitors understand their responsibilities when using college ICT systems and equipment.

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.	How do you intend to mitigate or eliminate any negative impact identified?

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

Name	
Mark Owen	Assistant Principal – Student Services
Mark Poole	Head of Estates
Jane Deery	Vice Principal - STEM

Equality Analysis Sign-Off Signature and Date:	18/09/2024
Review Date:	18/09/2025

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:

Emails, internet access, login details

Is data collected personal and/or sensitive?

Yes

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

Data is stored in a secure manner and access is restricted to only certain ICT Services Users. The data is periodically deleted.

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?

To comply with legal and JANET acceptable use policy. Also to ensure the college has robust security in place

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.

Informed in the Acceptable Use Policy and learning agreement.

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

To comply with the legal requirements and with JANET Acceptable Use Policy.

How will you ensure data quality and data minimisation?

Only necessary data is stored and deleted when not needed.

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 Wood

Date: 18/09/2024

Appendix 3: COMMUNICATIONS PLAN

TITLE OF COLLEGE POLICY: ICT Security Policy	**DATE APPROVED BY** Date: 12/03/2024

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

CHANNEL (select appropriate with √)					
Policy & Strategy Team (PST)		Quality Improvement Network (QIN)		Marketing team	
Meeting		Meeting		NC Update Intranet Website	
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