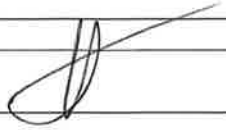
POLICY STATEMENT

TITLE:	**ICT Security Policy**
INTRODUCTION/OVERVIEW:	ICT Systems are used to support learning and to enhance knowledge. Computer Networks can be damaged by misuse, vandalism, Hacking, virus attacks and several other means, both locally and via the Internet.
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 and data 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.
QUALITY STATEMENTS:	• The ICT Services Team will provide a robust, secure ICT system environment and an appropriate security monitoring system. • The College reserves the right to use these systems where appropriate to monitor correct usage. • The ICT Services Team will provide appropriate back up for the ICT Systems. • Users of the ICT Systems are expected to observe security procedures when using the ICT Systems. • Disciplinary action may be taken against users not complying with the policy.
LINKED POLICIES/ PROCEDURES:	• ICT Acceptable Use Policies • Data Protection Policy • Any appropriate legislation including the PREVENT strategy 2011
MONITORING PROCEDURE:	• Deputy Principal For Finance and Corporate Affairs • ICT Operations Manager • Periodic Review
DATE FOR REVIEW AND NEXT DIVERSITY IMPACT ASSESSMENT:	April 2019
RESPONSIBILITY: **Overall (Directorate/Dept):** **Implementation:**	Deputy Principal For Finance and Corporate Affairs

ENDORSED BY:		**(Signature)**
Policy & Strategy Group / Corporation		**(Position)**
		(Date)

APPROVED:		**(Signature)**
Principal		**(Position)**
	3/5/18	**(Date)**

ICT Security Policy

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 external systems by College equipment and all use of the College's computer networks, email facility, website(s), intranet, third party cloud storage and Internet 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, data protection and EU General Data Protection Regulation (GDPR) aspects, the Policy covers the use of ICT systems not owned by the College or located on its property, but used by College students or staff for study or business purposes connected with the College.

Objectives

Northampton College seeks to protect its assets and reputation from loss and to provide a secure, safe 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 and data are secure against loss by theft, fraud, malicious or accidental damage, or breach of privacy or confidence.

The College is protected from damage or liability resulting from use of its facilities and data for purposes contrary to the law of the land or the College's Charter.

Legislation and Other Policy

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

Data Protection Act
EU 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.
Terrorism Act
Prevent Strategy

And any other relevant legislation, current or future.

Application of the Policy

Enforcement

- It is the specific responsibility of the Deputy Principal For 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.

Breach

- It is the duty of the Deputy Principal For Finance and Corporate Affairs, together with the ICT Operations Manager to take appropriate action to prevent breaches of the policy. Where such action is outside of the remit of Information Services, the Deputy Principal For Finance and Corporate Affairs or the ICT Operations Manager will notify the appropriate officer(s) of the College or appropriate authorities.

Review and Audit

The Deputy Principal For Finance and Corporate Affairs, together with the ICT Operations Manager is responsible for regular review of the policy in the light of changing circumstances. The College's Internal Audit Team has a brief to ensure that the Policy is appropriate for the protection of the College's interests.

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 Deputy Principal For Finance and Corporate Affairs or the ICT Manager.

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

Users of the Internet will also need to comply with the JANET Acceptable Use Policy which is available from http://www.ja.net/company/policies/aup.html

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 For Finance and Corporate Affairs, together with the ICT Operations Manager 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 Senior Management Team and advice from appropriate external bodies.

Registered Users

The following are eligible to register as users and must complete the appropriate AUP:

- 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 recommended by a Team Leader.
- Any person of another educational establishment, teaching on the premises.
- Any person authorised by the Deputy Principal For Finance and Corporate Affairs or ICT Operations Manager.

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 For Finance and Corporate Affairs or ICT Operations Manager.

With the exception of access to material intended for the general public, use of information systems and networks shall be restricted to registered users. The Deputy Principal For Finance and Corporate Affairs or Information Systems Manager, 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 as this is external to the firewall and does not pose a security threat. Tokens are available from the ICT Helpdesk and all users receive a paper with the password on and a statement outlining the user's responsibility as to what they can access whilst using the college Internet.

Operational Practice

It is the responsibility of the Deputy Principal For Finance and Corporate Affairs and ICT Operations Manager to attend too the following:

- Securing the integrity of data and software held and processed on the College's information systems.
- Robust backup and restoration facilities of all central systems.
- Securing the integrity of all data storage areas, servers & computers.
- Ensuring file stores of servers & computers are secure and do not contain inappropriate material, especially copyrighted material.
- In the event of a suspected security breach, enforcing appropriate restrictions to the service until confidence is restored.
- Provision of appropriate antivirus, anti-spyware and 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 and shared storage areas.
- Provision of an appropriate software update system for servers and computers.
- Provision of a central firewall blocking facility for both email and web access allowing the college to restrict inappropriate use and specific facilities and websites and restriction of Spam emails.
- 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 classroom 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 approved remote access software and in an approved manner.
- Ensuring any data accessed from non-college equipment both internally and externally is secured appropriately and not shared with any third party.

Damage or loss to equipment, software or data resulting from failure to observe this policy is deemed to be the responsibility of the defaulter.

Control of access to personal data is the remit of the Data Protection Officer, who will ensure that information about rights and responsibilities under the Data Protection Act (1998) is made available.

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 will be held responsible for any losses if considered irresponsible.

Monitoring/Logging

The Deputy Principal For Finance and Corporate Affairs or ICT Operations Manager, as appropriate, is 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 For Finance and Corporate Affairs, the ICT Services Manager or ICT Operations Manager, 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 For Finance and Corporate Affairs and ICT Operations Manager. The central record will be made available for inspection by personnel authorised by the Principal.

The Deputy Principal For Finance and Corporate Affairs or ICT Operations Manager, 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.

ICT Security Advice and Training

It is the responsibility of the Deputy Principal For Finance and 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 ICT Operations Manager or other nominated college staff will undertake this by:

- Delivering a short talk at staff inductions.
- Delivering short talks at other area's team talks.
- Publishing articles in Northampton College-Update and Managers Update.
- Publishing advice on the staff Intranet.
- Email reminders.
- Any other method as deemed appropriate.

It is College policy that good practice relating to security should be a concern of all ICT training. Documentation and publicity of ICT facilities shall contain relevant advice on good practice relevant to security.

Duties of ICT Services Staff

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

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

The Deputy Principal For Finance and Corporate Affairs, together with the ICT Operations Manager, as appropriate, is 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.