European Union
European
Social Fund

NOTTINGHAM COLLEGE

DOCUMENT DETAILS

Document Name:	Nottingham College Information Security Policy
Document reference	IT/COP/190705
Version	1.3
Issue Date:	July 2020
Review Date:	July 2021
Document Author	Drew Keavey
Document Owner	Jo Clifford
Applicability	All staff, volunteers and Governors of Nottingham College, all other parties under contract
Summary	The purpose of this document is to set out the policy for Information Security

DOCUMENT CONTROL

Version history			
Version	Date	Reason for release/version update	Issued by
1	5 June 2018	First draft	Michael Davies
1.1	5 June 2018	Minor amendments for consistency with other policies	Drew Keavey
1.2	5th July 2019	Amendments to capture technology and threat changes	Drew Keavey
1.3	29th June 2020	Updates to reflect move to OneDrive	Drew Keavey

DOCUMENT APPROVAL

Approving person/body	Job Role (where applicable)	Date Approved
Governing Body		22 July 2019
Governing Body		22 July 2020

COMMUNICATION

Date sent to OLT	
Date sent to Internal Comms	22/07/2020
Publication required on External Website?	Yes

CONTENTS

1. INTRODUCTION

The purpose of this Policy is to describe the procedures, processes and measures in place to ensure the secure and safe use of the College's network and information systems resources, and to protect College systems from unauthorised access or disclosure.

2. OBJECTIVE

The objective of the College's Information Security policy is to ensure that the College's network, information systems and information are adequately protected from adverse failures of security, integrity, availability and compliance with legislative and operational requirements. The objective can only be achieved by appropriate physical and technological measures, and adherence to this and other relevant policies.

3. RESPONSIBILITIES

Information Security is the responsibility of the College as a whole and consequently the responsibility of all members of staff and other authorised users. All users of networks and systems must ensure the security, integrity and confidentiality of all systems and information that they access or use.

The College complies with all relevant legislation that impact on networks, systems and information collection, processing and storage.

4. NETWORK AND INFORMATION SYSTEM ACCESS

Staff are allocated an individual network username and password. Generic login accounts are not normally provided except in specific circumstances where this is necessary due to the environment or systems being accessed.

Each individual is granted access to network systems and resources based on their role Users should only access or attempt to access resources granted to them by virtue of their system profile. If additional access is required, as a result of temporary employment arrangements or as the result of involvement in a specific project or piece of work, this can be sought through the ICT helpdesk, and will require the authorisation of the relevant supervisor or manager.

Individuals will be provided access to a 'home' drive, and any relevant departmental or shared file storage areas. Users are expected to store work in their home drive or relevant shared area. No data should be stored on a computer's local drive.

These 'home' drive and shared drives will be stored in the Microsoft Office 365 environment as OneDrive or Sharepoint file stores with legacy file shares being transitioned over time to

these store. Only data stored in sanctioned locations will be securely backed up by the ICT department's security backup procedures.

Access to the network by users requiring elevated or administration level access are protected by multifactor authentication and monitored to ensure they are being used appropriately.

Access to individual information systems that are not authenticated through network access will be granted by the system administrator of the information system. This is usually role-based access with permissions to only the modules, sub-systems or data that is required by the role. If additional access is required, this can be requested through the ICT helpdesk and may require further authorisation.

Where computers are shared by a number of staff, it is essential that individual users log-off before others use the computer. Users are responsible for all computer activity (including Internet access and emails) undertaken whilst logged in.

5. PASSWORDS

The College has updated its password policy. The new rules mandate a minimum password length of 8 characters and after 10 failed login attempts the account will be locked out for a duration of 60 minutes. The ICT team recommend using a pass phrase rather than a "complex" password.

In line with the National Cyber Security Centre the majority of staff will only have to change their password once a year. The system will prevent users reusing their most recent passwords to ensure a new password is used. A number of high-risk accounts will have a password policy that reflects their overall risk (This could mean changing their password more often or having a higher complexity requirement).

Passwords should not be written down or posted in a location accessible by others. Passwords should not be shared. If you suspect that someone else knows your password, then contact the ICT helpdesk immediately for advice.

The college will implement multi-factor authentication to accounts based on a risk assessment of the potential threat the account being compromised would represent.

6. PHYSICAL SECURITY

All computer devices should have an asset sticker which should not be removed. Adequate precautions should be taken to protect computers and peripherals against theft or accidental damage. Extra care should be taken of mobile devices which by their nature are more transportable. Mobile devices should not be left unattended, and should not be left in vehicles overnight. All mobile devices should be encrypted to protect data. Please refer to the College Mobile Device Policy for more information.

7. BREACHES AND INCIDENTS

A personal data breach is defined as a breach of security leading to the complete or partial destruction, loss, alteration, unauthorised disclosure of, or access to personal or sensitive data (as defined in the Data Protection Act and General Data Protection Regulation. This might include an event or action which compromises the confidentiality, integrity or availability of systems or personal data either accidentally or through deliberate act or lack of action or control.

Other incidents include where the security of a computer, a system, an application or the network has been compromised. This may be the result of internal or external activity. All such incidents should be reported to your supervisor, and to the ICT helpdesk immediately, and if there is a real or suspected personal data breach this should be reported to the Data Protection Officer who can be contacted via email: dataprotectionofficer@nottinghamcollege.ac.uk . Some data breaches are reportable to the Information Commissioner's Office, and must be reported within 72 hours of identification. Please refer to the Nottingham College Data Breach Management procedure.

8. COMPUTER HARDWARE AND SOFTWARE

All computer hardware and software should be procured through the College ICT team. Only computer hardware provided through ICT should be connected to the network. If you have other devices that you wish to connect please contact the ICT helpdesk in advance of attempting to connect to the network. The exception to this is the use of the College provided "Guest" wireless networks. These provide access via wireless connection but will only connect to the Internet not the College internal network. Should you have any queries on the best way to access services on your own devices please contact ICT services.

9. MALWARE, VIRUS PROTECTION AND CONTROL

Malware is a term that refers to various types of malicious software such as virus, Trojans, worms, ransomware and spyware. Malware can have minor impact such as interrupting a service or facility, or longer term significant and permanent harm to a system or network. Malware is often introduced through Internet downloads, attachments to email or transferred to systems from portable storage devices such as USB pen drives.

The College has implemented a range of software and hardware measures to protect the College infrastructure and systems from attack. These are managed by the ICT department, but some systems such as the operating system will update automatically (often in the background). Please do not interfere with these updates. If you discover a virus, or are unsure about any unusual activity on your computer then stop working and report the activity to the ICT helpdesk immediately.

10. PHISHING

Phishing is the name for a class of scam that uses an email claiming to be from the college or from some other source. The email will typically include a link to a site that will either contain malware or will attempt to get you to enter your logon credentials.

Spearphishing is a form of phishing where the email will also make use of some of your personal data to make the email seem more plausible.

The college has implemented a range of measures to prevent phishing attacks however these are rapidly updating attacks, and some may get through. You should always be wary of clicking links in emails that are not from internal accounts. If you have any concerns about an email contact the ICT helpdesk who can advise.

The college will put out regular communications relating to phishing which will include general signs to look for and any specific examples that have been seen. Please take note of the guidance and be vigilant at all times.

11. TERMINATION OF EMPLOYMENT

In advance of a member of staff leaving the College local management should make arrangements for the transfer of any necessary files and email folders. The ICT helpdesk can provide advice and assistance. Authorisation may be required.

The HR and ICT teams will use the relevant information systems to ensure that the user credentials and network access are removed in a timely fashion. System administrators of College information systems need to replicate this action.

12. DISPOSAL OF MEDIA AND EQUIPMENT

All computer and related hardware, data storage devices, hard discs, magnetic tapes and mobile devices should be securely disposed of through suitably certified organisations that comply with the Waste Electrical and Electronic Equipment (WEEE) Regulation standards. The ICT team will manage the secure disposal of obsolete equipment that has been taken out of service. CDs and DVDs used for the storage of data should be shredded before disposal.

13. POLICY AND LEGISLATIVE CONNECTIONS

The College policies and guidelines which should be reviewed in conjunction with this policy include:

- Data Protection and GDPR Policy
- Data Breach Management procedure
- Social Media Policy
- Freedom of Information Policy
- Data Retention & Disposal Policy
- Mobile Device Policy

- E-Safety Policy
- ICT Acceptable Use Policy
- Network Security Policy
- Archiving Policy
- Disciplinary Policy
- Safeguarding Policy

Relevant legislation includes:

- The Regulation of Investigatory Powers Act 2000;
- The Telecommunications (Lawful Business Practice), (Interception of Communications) Regulations 2000;
- The Communications Act 2003;
- Data Protection Act 2008/General Data Protection Regulation;
- The Human Rights Act 1998;
- The Defamation Act 1996 and the Equality Act 2010;
- Malicious Communications Act 1988;
- Computer Misuse Act 1990;
- Freedom of Information Act 2000,
- Road Traffic Act 1988

14. TRAINING & SUPPOPRT

The College has a rolling programme of training activities which can be accessed to all staff. The ICT helpdesk can provide advice and support on ICT related issues.