Policy/Procedure/Guideline Review

Policy/Procedure/Guideline:	Acceptable Use of IT Policy
Senior Manager Responsible:	Deputy Principal – Finance and Resources
Author:	Head of IT and Network Services
Approved By:	Senior Management Team
Date Approved:	20th September 2016
Next Review Date:	September 2018
Publication:	Nelson and Colne College Extranet Nelson and Colne College Website Lancashire Adult Learning Website Nelson and Colne College Moodle Lancashire Adult Learning Moodle
Changes Made:	Ensure policy addresses the Prevent Strategy

Purpose

This summarises the key responsibilities and required behaviour of ***all*** staff and students of the Nelson and Colne College computer and information systems.

Policy

All staff and students are required to adopt procedures and practices that ensure the security, integrity and protection of information created and held by Nelson and Colne College, and to abide by the College's rules for the use of computer systems.

Applicable statutory regulations

The management of information security and the use of computers at Nelson and Colne College are framed by UK legislation including:

- Data Protection Act (1998)
- Counter-Terrorism and Security Act 2015: Prevent Duty
- Regulation Of Investigative Powers Act (2000)
- Freedom Of Information Act (2000)
- Human Rights Act (1998)
- Computer Misuse Act (1990)

Rules for the Use of College Computer Equipment

1. You must not remove computer equipment from the College without permission from Head of IT Network Services or a member of the College's Senior Management Team.
2. You must not install unlicensed software or applications on Nelson and Colne College computers, servers, laptops or mobile devices.
3. You must not circumvent any security measures put in place to ensure the safe operation of computing equipment, information systems or communications equipment e.g. disabling anti-virus software, removing password protections etc.
4. You must not install or use any device or software on College IT equipment that subverts or bypasses security controls including monitoring and filtering.
5. You must adhere to the terms and conditions of all license agreements relating to any software installed on, or accessed by, College computers including restrictions for commercial use.

6. You may only access, modify, save or copy records or files and computer records where you have been given the authority and authorisation to do so
7. You must not create, access, transmit or download inappropriate, terrorist related or extremist materials, using the College's IT systems or network. The College has a statutory duty to take steps to prevent individuals being drawn into extremism and terrorism, and a duty to alert and report any attempted access to, or dissemination of, such inappropriate material.
8. You must comply with the JANET network Acceptable Use Policy (which can be found on the JANET's network website) when using an internet connection from or to the College including, but not limited to, the following examples:
    - Not engaging in harassing, defaming or other anti-social behaviours on-line
    - Not creating or transmitting any offensive, obscene or indecent images, data or other material in any form
    - Not using the network to attack or gain unauthorised access to other network, computer systems or data
    - Not transmitting unsolicited bulk email (spam)
    - Not infringing the copyright of another person or organisation
9. You must ensure that you log out of College systems at the end of each session
10. You must not leave open-access computers "screen locked" for more than 20 minutes, thereby preventing others from using the shared resource.

Passwords, ID and Access

Your unique User Identification code (User ID) and password are the primary control for access to the College's information systems, computer services and network. All access and activity that is logged can be tracked back to your user ID. Your User ID and password are for your sole use, therefore:

11. You must not use another person's user ID, nor permit or allow another person to use your user ID for any reason.
12. Your password must be kept confidential. You must not allow your password to become known by another person. Disclosing your password to someone unauthorised in order to gain access to an information system or computer service may be a disciplinary offence.
13. You must follow good security practices when selecting, using and protecting your passwords.

14. The IT helpdesk service can reset your password if required. We will never ask you to divulge your password – beware of emails, and phishing phone calls that ask you to disclose your password.
15. All Internet traffic passing through the College network, including email, is traceable through logs and is retained for set periods of time.
16. You must obtain explicit written and specific clearance from the College's Safeguarding Team before engaging in research with materials on-line that are: highly controversial; sensitive; could expose you to harm or undue attention; or potentially breach College policies. For example, extremist sites, terrorism or counter terrorism sites, pornographic material, criminal activity or activity which is likely to give rise to civil action against the College.
17. The College has a statutory duty to co-operate with Law Enforcement Agencies in the course of an investigation, allowing access to your email, file spaces and any logged information, where a warrant/request is properly executed in relation to an investigation.

Protection against malicious code

Viruses, spyware, hacking utilities etc. are classed as malicious code and are a risk to maintaining information security, therefore:

18. You must not deliberately, or through lack of care, allow malicious code or any other "nuisance" program or file onto any College systems. You must take the utmost care when downloading files from the internet or opening files attached to electronic mail.
19. You must ensure that any non-College equipment you use to access College systems is free of malicious code e.g. with an up to date anti-virus product
20. You must not deliberately circumvent any precautions taken to prevent malicious code accessing College systems e.g. by disabling antivirus software
21. You must take steps to secure your computer when leaving it for a few minutes to avoid the risk of interference or misuse e.g. by locking the screen.

Use of email and other electronic communication systems.

22. The College and staff will correspond with you by email using your nelson.ac.uk email address, regarding your study or on College business. You must check your College email regularly.
23. You must use your nelson.ac.uk email address when communicating with the College and staff so that your correspondence can be verified and tracked. Staff should not

respond to email from other email domains because of the difficulty of establishing authenticity.

24. You should not give serious attention to unsolicited email until and unless the sender's identity and authenticity of the mail have been verified

25. When attaching data files to an email that contains personal data i.e. data relating to living persons, e.g. for the purposes of research activity, the attachment must be encrypted.

Use of Mobile devices

26. You must take additional care when using mobile technologies to hold College data (including email) or access systems. Staff must ensure that they adhere to the additional controls and requirements set out in the *Information Security for Mobile Devices Policy.*

Leaving the College

27. When you leave the College, or suspend your study, your computer user account will normally be suspended.

28. You must make all efforts to transfer important files from your College file space before you leave the College.

Disciplinary Process

29. Use and Access to College resources and information is conditional upon adherence to the Acceptable Use of ICT Policy. Where there is found to have been a deliberate attempt at unauthorised access, or wilful neglect to protect the College information systems and data, the College will initiate the appropriate disciplinary processes.

30. In the event that you breach the terms within the Acceptable Use of IT Policy, your access to your user account may be suspended in order to allow an investigation to take place.

This Policy to be Read by:	
Staff	✓
Students	✓
Governors	
Consultants	
Partner staff of Nelson and Colne College	✓
Contractors of the College	