Policy/Procedure/Guideline Review

Policy/Procedure/Guideline:	Acceptable Use of IT Policy
Senior Manager Responsible:	Vice Principal, Chief Information Officer
Author:	Vice Principal, Chief Information Officer
Approved By:	Senior Management Team
Date Approved:	5th October 2021
Next Review Date:	5th October 2022
Publication:	Nelson and Colne College Group Staff Hub Nelson and Colne College Group Website Lancashire Adult Learning Website Nelson and Colne College Group Website Lancashire Adult Learning Nelson and Colne College Group Moodle
Changes Made: **Related College policies:**	Ensure policy addresses new legislation and organisational changes E-Safety policy Safeguarding policy Student behaviour Staff and student code of conduct

Purpose

This policy summarises the key responsibilities and required behaviour of all staff and students as regards the Nelson and Colne College Group technology 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 Group 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)
- The Public Sector Bodies (Website and Mobile Applications) (No. 2) Accessibility Regulations 2018
- Freedom of Information Act (2000)
- Human Rights Act (1998)
- Computer Misuse Act (1990)
- JANET Acceptable Use Policy

Introduction

Digital technologies have become a key part of our lives, both inside and outside of College. Safe use of these technologies is essential.

This acceptable use agreement is intended to ensure that:

- Students will be responsible users and stay safe when using the internet and other digital technologies for educational use.

- Staff will be responsible users and stay safe when using the internet and other digital technologies for educational use.

- School systems and users are protected from accidental or deliberate misuse that could put the security of systems at risk.

We expect staff and students to agree to be responsible users at all times.

Acceptable Use Agreement – Your obligations and expected behaviour

I understand that I must use College systems in a responsible way, to make sure there is no risk to my safety or to the safety and security of the systems and other users.

I will keep my username and password secure – I will not share it or try to use any other user’s user id and password.

I will not disclose or share personal information about myself or others when online.

I will report any unpleasant or inappropriate material or messages.

I understand that the College systems and devices are intended for educational use and that I will not use them for personal or recreational use unless I have permission.

I will not try to make large downloads or uploads which might take up internet or storage capacity and prevent others from carrying out their work.

I will respect others work and property and will not engage with others files, without the owner’s permission and knowledge.

I will be polite and responsible when I communicate with others.

I will not distribute images of others without their permission.

I will only use my personal devices in College in accordance with the standards and rules set out in this agreement.

I understand there are risks in accessing internet sites and information and I will not upload, download or access inappropriate material.

I will not use any programs to try to bypass the filtering and security systems put in place by the College to protect its staff and students.

I will not open any hyperlinks in emails or documents, unless I know and trust the person sending them.

I will not try to change any device settings or to install any software which is not approved by the College.

I understand that if I fail to comply with this agreement, I may be subject to disciplinary action.

The Policy Detail

1. Book all computer equipment through the standard booking procedures, completing a Consent Form, or gain permission from the CIO or the Desktop Services Team Leader, prior to its removal from College premises.

2. Installing unlicensed software or applications on Nelson and Colne College Group computers, servers, laptops or mobile devices is not permitted.

3. Remember, College equipment is to be used for College work or study purposes only. This includes laptops, tablets, MiFi units, telephones, mobiles phones, or any other equipment owned by the college which is in your care.

4. 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. Make sure you work within the security measures put in place to ensure the safe operation of computing equipment; these are there for your safety. This includes anti-virus software and password authentications.

5. Other devices or software on College IT equipment that subverts or bypasses security controls including monitoring and filtering are not allowed to be installed on any College owned equipment.

6. 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.

7. Access, modify, save or copy records or files and computer records only where you have been given the authority and authorisation to do so.

8. Always 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 online
   - 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. Remember to log out of College systems at the end of each session.

10. Remember to not leave open-access computers “screen locked” for more than 20 minutes and secure your computer when leaving.

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. Do not use another person's user ID, nor permit or allow another person to use your user ID for any reason.

12. Keep your password confidential. Don't allow your password to become known by another person. Follow good security practices when creating your passwords. Don't write them down and use highly secure passwords (using at least three of the following – numeric, lowercase, uppercase, symbol).

13. The IT helpdesk service can reset your password if required. We will never ask you to divulge your password.

14. On a work-related device, personal email addresses or accounts must not be used. They may only be registered or signed into work email addresses. All devices returned must be free of codes, etc. which would restrict access and redeployment.

15. 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:

16. You must take the utmost care and not deliberately, allow malicious code or any other "nuisance" program or file onto any College systems.

Use of email and other electronic communication systems.

17. College staff should use their nelsongroup.ac.uk email address when communicating so that correspondence can be verified and tracked.

18. College staff should encrypt all files containing personal data and take care when using mobile technologies to hold College information.

Leaving the College

19. When you leave the College, or suspend your study, your computer user account will normally be suspended. Any loaned equipment must be returned to the College.

Disciplinary Process

20. Use and Access to College resources and information is conditional upon adherence to the Acceptable Use of IT 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, which may include reporting to the Police.

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