IT Acceptable Use Policy and e-Safety Procedures

Title:	IT Acceptable Use Policy and e-Safety Procedures
Policy Number:	P027
Approval Date & Version:	March 2022, Ver. 1.0
Approved by:	Board of Governance (BoG)
Next Review Date:	January 2024

External Reference Points:

External Source	Reference Points
UKQC- Core Practices	N/A
UKQC- Advice and Guidance	N/A
Awarding Body Reference	N/A
Other reference Points Laws, Rules and Regulations	• Data Protection Act 2018 • Counter Terrorism and Security Act 2015
Other Reference Points: NCL Policies	• NCL: Safeguarding Policy • NCL: Master Information and Security Policy

This Policy is divided into two sections, namely:
Section A: IT Acceptable Use Policy
Section B: e-Safety Procedures

Section A: IT Acceptable Use Policy

1. Aim- IT Acceptable Use Policy

1.1. The aim of this policy is to ensure that the IT facilities of Nelson College London are used safely, lawfully and equitably.

1.2. The policy provides a framework for the use of IT resources available within the College.

1.3. The College seeks to promote and facilitate the proper and extensive use of '*Information Technology*' in the interests of learning, teaching, innovation and research, including business and community engagement partnerships.

1.4. The College also has a statutory duty, under Section 26 of the Counter Terrorism and Security Act 2015, termed "PREVENT". The purpose of this duty is to aid the process of preventing people being drawn into terrorism.

2. IT Acceptable Use Policy- Scope

2.1. Members of the College and all other users (staff, students, visitors and contractors) of the College's facilities are bound by the provisions of this policy.

2.2. This policy applies to anyone using Nelson College London IT facilities (hardware, software, data, network access, telephony, services provided by licensed third parties, online cloud services or using College IT credentials) including students, staff, contractors and third-party individuals who have been given access for specific purposes

3. IT Unacceptable Use

3.1. Subject to exemptions defined in section 3.6 of this policy, the College Network may not be used directly or indirectly by a User for the download, creation, manipulation, transmission or storage of:

3.1.1. any offensive, obscene or indecent images, data or other material, or any data capable of being resolved into obscene or indecent images or material;

3.1.2. unlawful material, or material that is defamatory, threatening, discriminatory, extremist or which has the potential to radicalise themselves or others;

3.1.3. unsolicited “nuisance” emails;

3.1.4. material which is subsequently used to facilitate harassment, bullying and/or victimisation of a member of the College or a third party;

3.1.5. material which promotes discrimination on the basis of race, gender, religion or belief, disability, age or sexual orientation;

3.1.6. material with the intent to defraud or which is likely to deceive a third party;

3.1.7. material which advocates or promotes any unlawful act;

3.1.8. material that infringes the intellectual property rights or privacy rights of a third party, or that is in breach of a legal duty owed to another party; or

3.1.9. material that brings the College into disrepute.

3.2. The College Network must not be deliberately used by a User for activities having, or likely to have, any of the following characteristics:

3.2.1. intentionally wasting staff effort or other College resources;

3.2.2. corrupting, altering or destroying another User’s data without their consent;

3.2.3. disrupting the work of other Users or the correct functioning of the College Network; or

3.2.4. denying access to the College Network and its services to other users.

3.2.5. pursuance of commercial activities (even if in support of College business), subject to a range of exceptions. [Please contact the Head of Administration & Resources to discuss your commercial needs.

3.3. Any breach of industry good practice that is likely to damage the reputation of the JANET network will also be regarded prima facie as an unacceptable use of the College Network.

3.4. Where the College Network is being used to access another network, any abuse of the

acceptable use policy of that network will be regarded as unacceptable use of the College Network.

3.5. Users shall not:

3.5.1. Introduce data-interception, password-detecting or similar software or devices to the College's Network;

3.5.2. seek to gain unauthorised access to restricted areas of the College Network;

3.5.3. access or try to access data where the user knows or ought to know that they should have no access;

3.5.4. carry out any hacking activities; or

3.5.5. intentionally or recklessly introduce any form of spyware, computer virus or other potentially malicious software.

3.6. Exemptions from Unacceptable Use:

3.6.1. There are a number of legitimate academic activities that may be carried out using College information systems that could be considered unacceptable use, as defined in sections 3.1-3.5 of this policy. For example, research involving defamatory, discriminatory or threatening material, the use of images which may depict violence, the study of hate crime, terrorism related material or research into computer intrusion techniques. In such circumstances advice should be sought from the College (if potentially illegal material is involved) and/or notification made to the Principal via the procedure outlined in the College's Prevent Policy.

3.6.2. Any potential research involving obscene or indecent material must always be discussed in advance with the College.

3.6.3. If a member of the NCL community believes they may have encountered breaches of any of the above, then they should make this known immediately to an appropriate College authority. The details of reporting process are available in Section B of this policy.

4. Consequences of Breach of IT Acceptable Use Policy

4.1. In the event of a breach of this '*IT Acceptable Use Policy'* by a '*User*' the College may in its sole discretion:

4.1.1. Restrict or terminate a User's right to use the College Network;

4.1.2. Withdraw or remove any material uploaded by that User in contravention of this Policy; or

4.1.3. Where appropriate, disclose information to law enforcement agencies and take any legal action against a User for breach of this Policy, including but not limited to claiming all costs, fees and disbursements (including but not limited to legal fees) connected therewith.

4.2. In addition, where the User is also a member of the NCL community, the College may take such action, disciplinary or otherwise as it deems appropriate and which is in accordance with its rules and regulations.

5. Monitoring and Evaluation

5.1. The effectiveness of the implementation of this policy will be monitored through PEG and Academic Board

Section B: e-Safety Procedures

1. e-Safety Procedures - Introduction

1.1. Nelson College London recognises the benefits of e-communication and is also aware of the potential risks and challenges associated with it. The main priority at Nelson College London is to make students and staff stay ***'e-Safe'***.

1.2. The College implements appropriate safeguards within its IT Systems to support students and staff to identify and manage risks independently and with confidence.

2. Security

2.1. Nelson College London ensures that the College network is safe and secure by implementing following measures:

2.1.1. security software is kept up to date.

2.1.2. enhanced filtering and protection of firewalls, servers, routers etc. are used to prevent accidental or malicious access of systems and information.

2.1.3. digital communications (including email and internet postings) over the College network are regularly monitored.

3. Roles and Responsibilities

3.1. '*Online Safety*' incidents are any instances where there is risk of harm, or actual harm, to an individual where digital technology has been used. (For example, indecent images, online abuse or illegal radicalisation).

3.2. All students must know what to do if they have online safety concerns and whom to report to. In most cases, this will be:

3.2.1. Personal Tutor / Programme Leader

3.2.2. Academic Managers

3.2.3. Welfare Managers/ Safeguarding Officers

3.3. Where a member of staff wishes to report an incident, they must contact their line manager as soon as possible.

4. Contact Details of Welfare/ Safeguarding Officers

4.1. The contact details of Welfare officers are as follows

- Tatiana Russell – HR/Health and Safety/Disability Support/Student Welfare Manager
  Email: t.russell@nelsoncollege.ac.uk
- Hira Khan- Administrator/Safeguarding/Disability Support/Student Welfare Officer
  Email: h.khan@nelsoncollege.ac.uk
- Lucia Ismail- Safeguarding/Disability Support/Student Welfare Officer
  Email: l.ismail@nelsoncollege.ac.uk

4.2. The Head of HR and the Head of Academic Services are the College's Designated Safeguarding Officers, respectively for staff and students.

The contact details of Head of HR: Athiqul Islam: a.islam@nelsoncollege.ac.uk

The contact details of Head of Academic Services: Aleksandra Osiniagova: osiniagova@nelsoncollege.ac.uk

5. Incidence and Response

5.1. The College will not tolerate any abuse of its IT systems. Any reported incident of online bullying, harassment or other unacceptable conduct will be treated seriously and in line with the rules, regulations and relevant student and staff disciplinary procedures.

5.2. Following any incident, the College will review what has happened and decide on the most appropriate and proportionate course of action. Sanctions may be put in place, external agencies may be involved or the matter may be resolved internally depending on the seriousness of the incident. Serious incidents will be dealt with by senior management, in consultation with appropriate external agencies and police will be informed if the incident is considered illegal.

6. Information for Students and Staff

Use of Images, Video and Audio:

6.1. The use of images photographs, video and audio is popular in teaching and learning and is encouraged in Nelson College London where there is no breach of copyright or other rights of another person (e.g. image rights or rights associated with personal data).

6.2. The College may record group tutorial / class sessions and share or distribute them online for the benefit of the students. However, no student(s) or a member(s) of staff is allowed to copy, share and distribute any photograph, video or audio clip of an individual or group without their consent.

6.3. The College also ensures that approved photographs, videos or audio clips do not include names of the individuals without their consent.

Personal Information:

6.4. All staff and students are responsible to keep their personal information safe and secure at all times.

7. Guidance and Training

7.1. The College undertakes all necessary measures to support staff and students to stay 'e-Safe' through the provision of guidance and training which enables individuals to identify risks independently and manage them effectively.

7.2. Guidance for Students:

7.2.1. Students are encouraged to question the validity and reliability of materials researched, viewed or downloaded. They are also encouraged to respect the copyright of other parties and to cite references properly.

7.2.2. In future *'Online Safety'* will form a part of the induction programme for new and returning students.

7.3. Guidance for Staff:

7.3.1. Existing staff are encouraged to familiarise themselves with the policies, rules and regulations of Nelson College London.

7.3.2. New staff will take part in online safety training as a part of their induction programme.