Nelson College London

# IT ACCEPTABLE USE POLICY

| | |
|---|---|
| **Approval Date & Version:** | January 2019, Ver. 0.4 |
| **Approved by:** | Board of Governance (BoG) |
| **Next Review Date:** | January 2020 |

## 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 | • Counter Terrorism and Security Act 2015 |

## 1. Introduction:

1.1. It is the responsibility of all users of Nelson College London’s IT services to read and understand this policy. This policy may be updated from time to time, in order to comply with legal and policy requirements.

1.2. This Acceptable Use Policy is taken to include IT network accessible through the College’s IT resources. 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.

1.3. Members of the College and all other users (staff, students, visitors, contractors and others) of the College's facilities are bound by the provisions of its policies in addition to this Acceptable Use Policy.

1.4. The College seeks to promote and facilitate the positive and extensive use of Information Technology in the interests of supporting the delivery of learning, teaching, innovation and research to the highest possible standards. This also requires appropriate and legal use of the technologies and facilities made available to students, staff and partners of the College.

## 2. Unacceptable Use:

2.1. Subject to exemptions defined in section 2.6 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:

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

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

2.1.3. Unsolicited “nuisance” emails;

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

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

2.1.6. Material with the intent to defraud or which is likely to deceive a third party;

2.1.7. Material which advocates or promotes any unlawful act;

2.1.8. 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

2.1.9. Material that brings the College into disrepute.

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

2.2.1. Intentionally wasting staff effort or other College resources;

2.2.2. Corrupting, altering or destroying another User's data without their consent;

2.2.3. Disrupting the work of other Users or the correct functioning of the College Network; or

2.2.4. Denying access to the College Network and its services to other users.

2.2.5. 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.

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

2.4. 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.

2.5. Users shall not:

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

2.5.2. seek to gain unauthorised access to restricted areas of the College's Network;

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

2.5.4. carry out any hacking activities; or

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

2.6. Exemptions from Unacceptable Use

2.6.1. 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 at 2a-e. 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 College Principal via the procedure outlined in the College's Prevent Policy if the material relates to the promotion of extremism/terrorism prior to the introduction of said material onto the College network.

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

2.6.3. If a member of the College community believes they may have encountered breaches of any of the above, they should make this known to an appropriate College authority (such as the College Principal or Director of Computing Services/Head of Resources).

## 3. Consequences of Breach:

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

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

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

3.1.3. 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.

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

## 4. Monitoring and Evaluation:

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