I.T Acceptable Use Policy - Final

Document SG3	
Policy owner:	Head of Safeguarding and Welfare (Lead DSL)
Policy Author	Head of Safeguarding and Welfare (Lead DSL)
Version	1.1
Review date	Last reviewed November 2021 Next review date November 2022
Links to College Strategy & College Values	Ambitious – support ambitions to meet aspirational targets for all Successful – help identify and address aspects of performance to reach excellence Professional - to focus on organisational development following learner feedback Innovation – to deliver an innovative experience for learners Respectful – to be inclusive and aware of diverse cultures, valuing our students, staff, and all Stakeholders Engaging – to support an inclusive approach to enable all learners to participate in learner engagement meetings, events, and activities to take on board feedback and be responsive to needs
Applies to:	All Staff, Contractors, Governors and Leaners
Monitoring and evaluation:	The arrangements for I.T Acceptable Use Policy monitoring are subject to continuous review as part of the College's data monitoring at Safeguarding Committees. The outcomes of the monitoring process will be reported to Governors at regular intervals via review of KPIs and reports.

Associated documents/policies for this area:

SG1	Safeguarding Young People and Vulnerable Adults
SG2	Prevent Strategy
HR	Staff and Corporate Code of Conduct

Purpose	The College seeks to promote and make easy the proper use of technology in the interests of communication, teaching and learning. Whilst the traditions of academic freedom will be fully respected, this also requires responsible and legal use of the technologies and facilities made available to the College.
Process & arrangements	**1.0 Scope** This policy covers appropriate use of I.T systems for staff and learners and applies to all employees operating on behalf of Newham College. This facilitates internal and external communication, and to provide access to information and materials on the internet. These systems are College property and are provided for the transaction of college business and are in line with our Safeguarding policy. **2.0 Policy** I.T Acceptable Use Policy (including social networking facilities). All College staff will be provided with a copy of this policy and will be required to sign the declaration at the back of this policy to show their acceptance of its terms. This form will then be retained on your Human Resources file. Staff will always be expected to comply with this policy. In any event, use of the systems is considered as consent to this policy and its content. This policy is underpinned by the key principles of the staff and corporate code of conduct. All learners receive an induction and IT Online Learning Module on E-Safety covering this policy and more. **2.1** Any breach of this policy may result in disciplinary action, which might, depending on the circumstances, include dismissal. A breach or suspected breach of policy by college staff, contractor, partners, or learners may result in the temporary or permanent withdrawal of College ICT (Information Communication Technology) hardware, software, or service. Policy breaches may also lead to criminal or civil proceedings. **3.0 Personal use** College I.T systems and the use of e-communication is primarily for work-related purposes and telephone; computer and e-mail accounts are the property of the College and are designed to assist in the performance of your work. Whilst the College will attempt to respect your privacy, you should have no expectation of privacy in any e-mail sent or received, whether it is of a business or personal nature, or in any telephone calls data logged incoming and outgoing. **4.0 Use of the College e-communications** E-mails should be drafted with care. Due to the informal nature of e-mail, it is easy to forget that it is a permanent form of written communication, and that material can be recovered even when it is deleted from your computer. The College places a disclaimer at the end of outgoing emails to disassociate itself from the email content. **4.1** You should not send unnecessary emails or copy other recipients into the message without good reason. Unnecessary emails waste colleagues' time and congest the email system. You should regularly delete e-mails to prevent over-burdening the system. The 'All Staff' address facility is only to be sent from the College Clerk, Director of HR, Deputy Principal, Chief Operating Officer and The Principal and CEO.

4.2 All staff have College email in the form of name@newham.ac.uk accounts for effective communication between the College, tutors, and peers. Learners and staff agree the I.T Acceptable Use Policy when logging onto the College computers.

4.3 You must not use the College's e-communication systems to send or view any materials that might cause offence to any person by reason of: See the Safeguarding, Prevent Strategy and the Equality and Diversity policy

- any sexually explicit content
- remarks relating to a person's sex, race, disability, sexual orientation, gender
- reassignment, religion, belief, political beliefs, age, ethnic origin, colour or nationality
- Any other materials that you believe are offensive, illegal, immoral, or contrary to public policy.
- Any material that is a breach of the 'Prevent Duty' and the college Prevent Strategy.

4.4 You must not send chain letters via the electronic mail, including joke or "good will" emails. These systems are used to gather email address which are then sold. If you receive virus warnings or chain letters via email, or receive anything that is questionable or illegal, then please contact the College's IT department as soon as possible.

4.5 Subscription to Internet mailing lists should be limited to those related to your work in the College.

4.6 The College reserves the right to block what it considers unnecessary or inappropriate websites or downloads and any attempts to disable, defeat or circumvent any of the College's computer security facilities will constitute gross misconduct.

4.7 You must not download software which requires a licence. Software requests should be made to the IT departments. College staff or learners should not download or install any additional software or introduce non-text files or unknown messages on to the College's system. You must not take any copies of software on the College's system for your own unless agreed with the IT department and your line manager, this must also be in writing.

5.0 Use of Public e-communications Whilst the College recognises staff and learners rights to a private life, during any use of social networking sites, or maintenance of personal blogs (online diaries), you are required to refrain from making any reference to the College that could bring it into disrepute. You must not make negative, derogatory, or defamatory remarks in e-communications about staff, learners, competitors, or any other person. Any such remark could result in legal action against you and/or the College. The College will consider any personal information that staff and leaners make available on networking sites or blogs to be in the public domain. Staff should ensure that any such information does not bring the College or its reputation into disrepute

6.0 Copyright and Downloading Copyright applies to all text, pictures, video, and sound, including those sent by e-mail or on the Internet. Files containing such copyright protected material may be downloaded, but not forwarded or transmitted to third parties without the permission of the author of the material or an acknowledgement of the original source of the material, as appropriate. If you copy, amend, or distribute any such material without the copyright owner's consent, you could be sued for damages by the copyright owner.

7.0 General Computer Usage you are responsible for safeguarding your password for the system. For reasons of security, your individual password should not be printed, stored online, or given to others, including family members/friends. User password rights given to you should not give rise to an expectation of privacy. You must change your password when prompted. The College will not be liable for any loss of files if you do connect your personal or work laptop to the network.

8.0 Teaching and Learning using Technologies (including social networking sites) Blocking and banning social networking sites limits exposure to risk but is not always suitable or beneficial to tutors or learners. Informal learning using social networking facilities is a 'way of life'. It is our policy to empower our staff and learners. The College provide a network account, safe storage, a virtual learning environment using MOODLE VLE, and Microsoft Office Package, including forums and 'Teams.'

8.1 The College permits the use of innovative technologies and facilitates learners' need to use social network software such as YouTube, Wikipedia, Facebook, blogs, and Google online applications to enhance their learning experience. Tutors are also permitted to use social network (web 2.0) technologies for teaching and learning.

8.2 It is important that learners learn how to be safe when they are using technologies, particularly Web 2.0 collaborative technologies such as social networking sites. The risks are often characterised by the four 'Cs'.

- **Content** - may be unsuitable or potentially illegal.
- **Contact** - this may be unwelcomed or inappropriate contact, it could be grooming or sexual contact
- **Conduct** - this could be as a recipient or as an active participant - giving out too much personal information or the bullying of another person.
- **Commerce** - this could be phishing or other methods of identity theft.

Students and staff will be trained in prevent awareness as per the Prevent Duty' and college 'Prevent Strategy'.

8.3 Tutors deploying social networking facilities for learners are responsible for ensuring learners are trained in e-safety and must cover the four 'Cs'. This programme will be made available to all tutors. Attendance to the College safeguarding training is mandatory for all staff.

8.4 Any teaching and learning materials should be uploaded to the College MOODLE or SharePoint and linked to from the external site e.g., Teams

8.5 Staff should not publish any material about any other person within the College community without their prior agreement including images.

8.6 Do not assume that any information acquired from the Internet, for which you may use for teaching material, is up-to-date and/or accurate or copyright free.

	8.7 All teaching staff are expected to incorporate e-Safety activities and awareness within their curriculum programme. Staff will receive appropriate I.T/E-safety and Prevent training.
Monitoring	part of their induction, new staff members, including agency staff, will always be made aware this policy and asked to ensure compliance with these procedures. Records of the staff nature will be kept by HR with regular reporting as part of staff compliance to Governors and Safeguarding Committee. staff and learners are made aware through inductions that the College monitors its firewalls d keystrokes using Barracuda and Impero web filters and searches. The Director for IT and ad of Safeguarding (Lead DSL) monitor all staff activity and the Deputy DSL's and feguarding Administrator monitors student activity. e Prevent Duty and college Prevent Strategy is reviewed annually, and the Prevent Risk sessment checked regularly through each term. is policy will be reviewed annually at the Safeguarding Committee meetings.

Staff declaration of understanding and agreement, as an employee of Newham College I have read and understood the I.T Acceptable Use Policy of the College and I hereby agree to abide by this policy.

Name: .....(Please print)

Signed: ..... Date: ...