IT ACCEPTABLE USE &

SOCIAL MEDIA POLICY

2024/2026

Version Control			
Author:	HE Quality Officer	Approved by:	Senior Leadership Team
Date Approved:	June 2024	Next Review Date:	June 2026
Responsible for review:	*Assistant Principal*	Version Number:	1
Version Amendments			
Date of Amendment:		Amendments:	
Date of Amendment:		Amendments:	

If you require this document in an alternative format, please contact HE Quality Officer via hequality@tameside.ac.uk (phone 0161 908 6763)

Contents

Introduction

1.1. This IT Acceptable Use Policy outlines the responsibilities and required behaviour of users of Tameside College's business systems, network infrastructure and computer systems.

Scope

2.1. This policy applies to all Tameside College employees, students, and third-party contractors (hereafter referred to as 'you').

2.2. This policy applies to all users of Tameside College's (our) network infrastructure and business system data, in whatever form, relating to business activities worldwide, and to all information handled by Tameside College (us) relating to other organisations with whom it deals.

2.3. This policy also covers all IT and information communications facilities operated by Tameside College (us) or on our behalf.

Purpose

3.1. This IT Acceptable Use policy sets out:

- your responsibilities as users of our business systems, network infrastructure and computer systems;
- our responsibilities to you as users of our business systems, network infrastructure and computer systems;
- our social media policy.

3.2. We may bring disciplinary action against you under the Values and Behaviours or relevant staff Disciplinary Procedure if you do not comply with the terms outlined in this IT Acceptable Use policy.

Support

4.1. IT Services can provide further guidance regarding the IT Acceptable Use Policy. Please contact the Helpdesk on 0161 908 6680 or helpdesk@tameside.ac.uk.

Policy principles

Computer/Device Access Control

5.1. Access to Tameside College's IT systems is controlled using Active Directory.

5.2. You will be given clear direction by Line Managers/Tutors on the extent and limits of your authority about Tameside College's business systems and confidential data. Training will be given to staff during Staff Induction sessions.

5.3. Through the tutorial provision students will be offered online safety information and training to enable them to develop the required knowledge and skills to recognise online risks and to keep themselves safe while working online. They will also be made aware of the filtering and monitoring arrangements that are in place at college, which aims to eliminate students' exposure to risks.

User IDs

5.4. A unique user ID and password will be assigned to you for your individual use.

5.5. You are accountable for all your actions whilst using Tameside College's network, business systems and data.

5.6. No other person than you must use your network account. However, IT Services may need to access your account for troubleshooting technical issues, security maintenance, data backup and recovery, etc.

Network Accounts:

5.7. We will assign your network account a unique password. You must not disclose this password to any other person. You will have to change your password at first login.

5.8. All passwords need to meet the following criteria;

- at least 8 characters in length.

- at least one numerical value.
- At least one capital letter.

5.9. You must take steps to protect your network account from unauthorised use. For instance, never write your password down on a 'Post it' note and stick it to your laptop case.

5.10. If you suspect your account may have been compromised, you must report this to IT Services immediately. You can contact the IT Helpdesk on 0161 908 6680 or helpdesk@tameside.ac.uk.

Email Addresses:

5.11. You will be assigned a unique email address for your individual use.

5.12. Some users may be granted additional access to use one or more generic email addresses.

5.13. You are not permitted to use Tameside College email addresses assigned to other individuals without their explicit permission (e.g., during handover, security concerns or delegation of responsibilities such as a personal assistant, etc).

Unacceptable Use:

5.14. You must not:

a) Allow anyone else to use your network account details on any Tameside College IT system.

b) Leave your user accounts logged in at an unattended and unlocked computer.

c) Use another user's network account to access Tameside College's business systems.

d) Leave your password unprotected (for example writing it down).

e) Perform any unauthorised changes to Tameside College's IT systems or information.

f) Attempt to access systems/data that you are not authorised to use or access.

g) Exceed the limits of your authorisation or specific business need to interrogate the system or data.

h) Connect any non-Tameside College authorised device to the Tameside College network or IT systems.

i) Store confidential Tameside College data on any personal laptop, smartphone, and tablet.

j) Store confidential Tameside College data on a personal USB stick or external hard drive.

k) Give or transfer Tameside College data or software to any person or organisation outside Tameside College without the authority of Tameside College.

l) Move any IT equipment without the permission of the IT Services Department. (Excluding mobile devices such as laptops and tablets).

Bring Your Own Device (BYOD)/College Network

5.15. Staff and students are allowed to connect personal devices (BYOD) to the College's 'TC Student Access' and 'TC Staff Access' wireless networks only.

Internet and Email Conditions of Use

5.16. Use of Tameside College's internet and email systems are solely for business and/or educational use, except for the conditions listed below.

5.17. Personal use will only be permitted where such use:

- does not affect your business/educational performance;
- is not detrimental to Tameside College in any way;
- is not in breach of any terms and conditions of employment or Learner Agreement.
- does not place you or Tameside College in breach of statutory or other legal obligations.

Unacceptable Use:

5.18. You must not:

a) Use the internet or your email account for the purposes of sending unsolicited messages, including the sending of 'junk mail' or messages that are harmful or abusive.

b) Use profanity, obscenities, or derogatory remarks in communications. This is in accordance with our College Values and Behaviours.

c) Access, download, send, or receive any data (including images), which Tameside College considers offensive in any way, including sexually explicit, discriminatory, defamatory, libellous, or illegal material. For more information see the college values see policies and reports page for FE students and policies page for HE students.

d) Create access, store, or transmit any material which promotes terrorism or violent extremism, or which seeks to radicalise individuals to such causes. This is in accordance with our Prevent policy, please see Tameside College Prevent Policy.

e) Use the internet or email to make personal gains or conduct a personal business.

f) Use the internet or email to gamble.

g) Use the email systems in a way that could affect its reliability or effectiveness, for example distributing chain letters or spam.

h) Place any information on the Internet that relates to Tameside College, alter any information about it, or express any opinion about Tameside College, as if they are those of the college, unless they are specifically authorised to do this.

i) Send unencrypted sensitive or confidential Tameside College data externally.

j) Forward Tameside College related data on email to personal (non-Tameside College) email accounts (for example a personal Hotmail account).

k) Make official commitments through the internet or email on behalf of Tameside College unless authorised to do so.

l) Download copyrighted material such as music media (e.g., MP3) files, film, and video files (not an exhaustive list) without appropriate approval.

m) In any way, infringe any copyright, database rights, trademarks, or other intellectual property.

n) Download or attempt to install any unapproved software from the internet without prior approval of the IT Services Department.

o) Connect Tameside College devices to the internet using non-standard connections.

p) Use third party proxy avoidance (VPN) software or browser plugins to bypass network security.

Clear Desk and Clear Screen Policy

5.19. In order to reduce the risk of unauthorised access or loss of information, as per our FE student's Data Protection policy and our HE student's Data Protection policy, Tameside College enforces a clear desk and screen policy as follows:

a) Personal or confidential business information must be protected using security features provided for example secure print on printers.

b) Computers must be logged off/locked or protected with a screen locking mechanism controlled by a password when unattended.

c) Care must be taken to not leave confidential material on printers or photocopiers.

d) All business-related printed matter must be disposed of using confidential waste bins or shredders.

Working Off-Site

5.20. It is accepted that Tameside College-owned laptops and mobile devices will be taken off-site. In accordance with our FE student's Data Protection policy and our HE student's Data Protection policy, the following controls must be applied:

a) Equipment and media must not be left unattended in public places and not left in sight in a vehicle.

b) Laptops must be carried as hand luggage when travelling.

c) Information should be protected against loss or compromise when working

remotely (for example at home or in public places).

d) Care should be taken with the use of mobile devices such as laptops, mobile phones, smartphones, and tablets. They must be protected at least by a password or a PIN and, where available, encryption.

Mobile Storage Devices

5.21. Mobile devices such as memory sticks, CDs, DVDs, and removable hard drives must be used only in situations when network connectivity is unavailable or there is no other secure method of transferring data.

5.22. You must never use these methods when transferring confidential data.

IT and Academic Misconduct

5.23. As part of the marking process the college uses detection software to identify academic misconduct. Full details of this can be found in the HE Acceptable Behaviour Policy, HE Academic Misconduct Policy including the procedures that underpin the academic misconduct policy principles which all students are expected to follow.

Software

5.24. You must only use software that is authorised by us on Tameside College's computers.

5.25. Authorised software must be used in accordance with the software supplier's licensing agreements.

5.26. All software on Tameside College computers must be approved and installed by the Tameside College IT Services department.

Unacceptable Use:

5.27. You must not store personal files such as music, video, photographs, or games on Tameside College IT equipment.

Viruses

5.28. The IT department has implemented centralised, automated virus detection and definition updates within Tameside College.

5.29. All workstations, physical and virtual servers have antivirus and anti-ransom software installed to protect the network from potential attacks.

Unacceptable Use:

5.30. You must not:

a) Remove or disable anti-virus software.

b) Attempt to remove virus-infected files or clean up an infection, other than using approved Tameside College anti-virus software and procedures.

Telephony (Voice) Equipment Conditions of Use

5.31. Use of Tameside College voice equipment is intended for business use only.

5.32. You must not use Tameside College's voice facilities for sending or receiving private communications on personal matters, except in exceptional circumstances.

5.33. All non-urgent personal communications should be made at your own expense using alternative means of communication.

Unacceptable Use:

5.34. You must not:

a) Use Tameside College's voice for conducting private business.

b) Make hoax or threatening calls to internal or external destinations.

c) Accept reverse charge calls from domestic or international operators unless it is for business use.

Social Media Policy

Policy Principles

6.1. At Tameside College, we recognise the importance of social media in the modern world and encourage our students and staff, to engage with these platforms responsibly and in line with our college values.

6.2. This policy applies to all social media interactions involving college staff, third-party contractors, students, or references to the college across various platforms, including but not limited to X (formerly Twitter), Facebook, LinkedIn, blogs, Instagram, YouTube, and others.

Behaviour when posting online

6.3. If you are posting to social media in your capacity as staff of Tameside College, you are expected to adhere to the principals of this policy when using social media in connection with your work.

6.4. Tameside College policies and regulations apply to behaviour in online/virtual spaces as they do in physical space. We will not tolerate behaviours such as cyberbullying, trolling, harassment, hate speech, collusion, cheating, and posting offensive or discriminatory content. Such actions may damage the college's reputation or threaten the safety of our community and will be subject to disciplinary action (staff) and acceptable behaviour Policy (Students).

Online Conduct

6.5. Students who contravene this policy will be referred to the HE Acceptable Behaviour Policy or FE College Values Behaviour.

6.6. Staff and third-party contractors of Tameside College who contravene this policy will be dealt with under the staff disciplinary policy.

6.7. You can use social media to discuss your personal experience or express critical views appropriately. You should not, however, expect any points raised on social media to be

addressed by Tameside College. In these instances, you may wish to consider raising your concerns via the (FE Customer Care Procedure, HE Complaints Policy).

6.8. There is no compulsion for you to engage on social media should you wish not to. Likewise, do not compel others to engage with you on social media.

6.9. If you set up or administer an unofficial social media group in relation to your work or studies with Tameside College (e.g., WhatsApp), you are encouraged to establish community guidelines that can be shared and understood by all.

Digital Communications

6.10. Digital communications between staff or third-party contractors and students should only be via official Tameside College email addresses and not via social media.

6.11. Tameside College hosted forums are for free and open academic discussion (within the bounds of the HE College Charter and FE College Charter. Posts or opinions from a Tameside College hosted forum should not be shared outside of Tameside College.

6.12. You must not comment on a named individual who belongs to Tameside College (either as staff or student).

6.13. You must not share Tameside College copyrighted materials without permission, and where permission is given, you must credit the source.

6.14. Recordings or extracts of recordings of tutorials (face-to-face or online) must not be shared on social media.

6.15. Answers to assessment questions and feedback must not be shared on social media. Please see the HE Academic Misconduct policy.

Tameside College Logo

6.16. The Tameside College logo may only be used on its own official social media accounts and groups. It must not be used for any other groups or accounts. Should you wish to use the logo for social media, requests should be sent to Marketing department 0161 908 6600.

Reporting matters of concern on social media

6.17. For more information of how to report a matter of concern or safeguarding matter on social media please refer to the Safeguarding at Tameside College page on the college website or the HE Safeguarding page, safeguarding@tameside.ac.uk.

Data Protection

7.1. Data protection, privacy and copyright legislation must be observed.

7.2. We recommend you check your privacy settings to consider how much information you are sharing.

7.3. Be cautious about sharing personal information that could be used to steal your identity (e.g., date of birth).

7.4. Never share your Tameside College login information or passwords.

7.5. Unless you have been given express permission to do so by Tameside College, be careful not to post anything that makes you appear to be speaking on behalf of Tameside College. It must be explicit that your views are your own.

Actions upon Termination of Contract/End of Studies

8.1. All Tameside College equipment and data, for example laptops and mobile devices including telephones, smartphones, USB memory devices and CDs/DVDs, must be returned to Tameside College at termination of contract/end of studies with Tameside College.

8.2. All Tameside College data or intellectual property developed or gained during the period of employment or study remains the property of Tameside College and must not be retained beyond termination or reused for any other purpose.

8.3. Staff email accounts will remain active for 30 days following termination of employment. Head of Department, student accounts and SLT accounts are retained for 6 months.

Monitoring and Filtering

9.1. All data that is collected is stored in line with the Tameside College Data Protection

Policy.

9.2. IT system logging will take place where appropriate, and investigations will be commenced where reasonable suspicion exists of a breach of this or any other policy. Tameside College has the right (under certain conditions) to monitor activity on its business systems, including internet and email use, to ensure systems security and effective operation, and to protect against misuse. Screens will be monitored using software by IT Services Staff and within classrooms by tutors.

9.3. Any monitoring will be carried out in accordance with audited, controlled internal processes, the Data Protection Act 2018, the Regulation of Investigatory Powers Act 2000, and the Telecommunications (Lawful Business Practice Interception of Communications) Regulations 2000.

9.4. It is your responsibility to report suspected breaches of security policy or confidential data immediately to your line manager, tutor, the IT Services department, or the MIS department. You can contact the IT Services Helpdesk by telephone 0161 908 6680 or email helpdesk@tameside.ac.uk.

9.5. All individuals are accountable for their actions on the internet and email systems.

Policy Compliance

Compliance Measurement

10.1. The IT Services Team will verify compliance to this policy through various methods, including but not limited to periodic walkthroughs, internal and external audits, and inspection and will provide feedback to the policy owner and appropriate manager.

10.2. The IT Services Team must approve any exception to the policy in advance. You can contact the IT Services Helpdesk by telephone 0161 908 6680 or email helpdesk@tameside.ac.uk .

Non-Compliance

10.3. If you are found to have violated this policy, you may be subject to disciplinary action for more information please see the college Disciplinary Procedure which can be found on the staff directory on MS Teams.

Glossary

Active Directory: Active Directory (AD) is a database and set of services that connect users with the network resources they need to get their work done.

Business Systems: Business systems refer to the interconnected and integrated set of processes, procedures, technologies, and resources that are designed to achieve specific business objectives or support the operations of an organization.

Cyberbullying: Cyberbullying is the use of technology to harass, threaten, embarrass, or target another person. Online threats and mean, aggressive, or rude texts, tweets, posts, or messages all count. So does posting personal information, pictures, or videos designed to hurt or embarrass someone else.

Non-standard connections: Non-standard connections refer to any method of linking or integrating systems, devices, or components that deviates from widely accepted or conventional standards. In technology, standards are established guidelines or protocols that ensure interoperability, compatibility, and reliability across different hardware or software platforms.

Related documents

Computer Misuse Act 1990

The Data Protection Act 2018

The Copyright, Design and Patents Act 1998,

Criminal Justice and Public Order Act 1994.

JANET Acceptable Use and Security Policies.

Counter-Terrorism and Security Act 2015.