BRIDGWATER & TAUNTON COLLEGE

IT ACCEPTABLE USE POLICY

Applicable to all students and staff

Author:	Head of Digital Transformation
Approved by:	SMT
Date:	June 2024
Review date:	June 2026

Contents

1. Introduction

1.1 The College requires all users of the organisations 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. Users will be presented with the agreement when they first logon to the College's network. The date they agree to the policy is logged into a database.

1.2 This Acceptable Use Policy is intended to provide a framework for use of the College's I.T. resources. It should be interpreted such that it has the widest application and so as to include new and developing technologies and uses, which may not be explicitly referred to.

1.3 In the event of a breach of this Acceptable Use Policy by a user the organisation may restrict or terminate a user's right to use the College network, disclose information to law enforcement agencies, withdraw or remove material uploaded by that user in contravention of this policy and the user be subject to disciplinary action, not excluding legal action.

2. Policy Statement

2.1. The College takes issues of safeguarding of young people and vulnerable adults very seriously. Users are asked to read and agree to the IT Acceptable Use Policy before using our IT systems.

3. Scope

3.1 The Policy applies to anyone using the College network and resources, including all staff, students and visitors.

4. Agreement

I will:

Comply with laws concerning computer use, including hacking, data protection, terrorism and copyright, and report any unpleasant, offensive, threatening or inappropriate material or messages/emails.

Keep my password safe and not allow another to use it, and only use my own password and not try to access another person's account or user another person's account.

Use a password that is not obvious to others, for example three random, memorable words.

Lock my computer when I am away from my desk so others cannot use it.

Treat all IT staff, equipment and services with respect.

Communicate with others in a professional manner and not use aggressive or inappropriate language.

Use College rather than personal systems (e-mail, social media etc.) for communication between staff and students.

Only use chat and social networking sites in College in accordance with the College's policies.

Ensure I know and trust the sender of an e-mail before opening it.

Agree to use Multi-Factor Authentication (MFA) to access systems

Ensure I have saved any work created to either OneDrive for Business, or

an appropriate file server so that the work is backed up and recoverable.

I will not:

Install any viruses, software or games onto the system, attempt to bypass filtering and security systems, or attempt to alter any computer settings, or use College IT systems for on-line gaming, gambling or peer-to-peer file sharing.

Use unlicensed copies or “pirated” versions of software.

Attempt to download or view illegal or distressing material, or material which has the potential to incite hatred or promote extremism.

Copy online material and claim it as my own work.

Engage in any activity which may use up network bandwidth and prevent others from being able to carry out their work.

Use the email system to send inappropriate messages, bully, harass, intimidate or send junk email to multiple users.

Disclose or share personal information about myself or others when online, or take and/or distribute images of anyone without their permission.

Store personal information or documents, including photographs and music, on College IT equipment. Such items may include, but are not limited too items such as scans of passports, bank details, credit/debit card information, scans of driving licences or other personal documents that may pose a risk if lost or stolen.

Attempt to circumvent any of the College's security systems, or attempt to elevate the privileges of any user account.

Use portable storage, such as external hard disks or USB memory sticks as they pose a security risk.

Surveillance and Monitoring, Policy Summary and Agreement to the Code:

I understand that the College reserves the right to monitor communication on its networks, especially if there is evidence of illegal or serious misuse of facilities. This means all web browsing, email logs, chat messages and attachments and telephone communications (landline or mobile) may be subject to scrutiny.

In line with the Government's Prevent Strategy, access to, or the creation and sharing of, material relating to violent extremism is prohibited and illegal. This includes racist and hate material, and material that promotes violence or attacks on individuals or institutions on the basis of religious, racial or gender grounds, or seeks to radicalise others. Using college computers to email terrorist publications to others constitutes a criminal offence.

I understand that the rules set out in this agreement also apply to use of College ICT systems used outside College (e.g. Office 365, iPads, laptops, Horizon, and Blackboard).

The College does not take responsibility for any problems a user experiences on their home/personal computer as a consequence of using remote college systems such as Office 365, or from the use of portable drives and/or portable storage devices.

I understand that if I fail to comply with this Acceptable Use Policy I will be subject to disciplinary action. This action may include loss of access to the network, email and/or Internet, suspension or exclusion from the College, and, in the event of illegal activities, involvement of the police. I understand that the College ICT systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by the College.

Data Access

Bridgwater and Taunton College respects the privacy of staff and students, however, the electronic data residing on College systems is the property of the College. The intellectual property rights for any work created by staff in their role belongs to Bridgwater and Taunton College. In rare instances, the College will exercise its right to access and/or audit this data.

Any Data or Audit search should be carried out for a justified business reason. Searching for information, data, audit logs, etc. without a plausible reason is strictly forbidden and will be considered under the College's Disciplinary Policy and Procedures.

The Head of Digital Transformation will monitor all data and audit searches and report any concerns to the Vice Principal – Finance & Resources.

BY LOGGING ON TO OUR NETWORK YOU AGREE TO ABIDE BY OUR ACCEPTABLE USE POLICY

5. Review of Policy

This Policy will be reviewed again in March 2025, unless the need arises sooner.