ACCEPTABLE USE OF INFORMATION TECHNOLOGY

This policy is available on-line at: www.tynecoast.ac.uk

- We will consider any request for this policy to be made available in an alternative format or language. Please contact: Head of Student Services.

- We review our policies regularly to update them and to ensure that they are accessible and fair to all. We welcome suggestions for improving the accessibility or fairness of this policy.

- All our policies are subject to equality impact assessments*****. We are always keen to hear from anyone who wishes to contribute to these impact assessments. Please contact: Head of Student Services.

*Equality Impact Assessments are carried out to see whether the policy has, or is likely to have, a negative impact on grounds of: age, disability, gender reassignment, pregnancy and maternity, race, religion or belief, sex or sexual orientation

Approved by:	**Version:**	**Issue Date:**	**Review Date:**	**Contact Person:**
SEG & JCC	**v.7**	**November 2019**	**November 2022**	**Business Operations Manager**

Equal Opportunities: **Impact Assessed**

POLICY NUMBER 2

ACCEPTABLE USE OF INFORMATION TECHNOLOGY

1 Policy Statement

This policy sets out the regulations for the use of the College's IT facilities to ensure best functioning and availability of the facilities for their stated purposes. Furthermore, these regulations are partially based on the model provided by the Universities and Colleges Information Systems Association (UCISA) and, as such, satisfy the requirements for connection to the Joint Academic Network (JANET).

The College has provided computers as an important tool for teaching, learning and administration. Use of College computers, by both members of staff and learners, is governed at all times by the following policy. All staff should understand their responsibilities under this policy, and direct any questions or concerns to the IT Helpdesk in the first instance.

Please note that use of the College network is intended to be as permissive and flexible as possible under current UK legislation and DfE guidelines. This policy is not intended to arbitrarily limit the ways in which you can use the system, but to ensure compliance with the legal responsibilities of the College and staff, to safeguard the reputation of the College, and to ensure the safety of all users.

Please respect these guidelines, many of which are in place for your protection.

2 Scope

This policy applies to any computer or communications equipment that is used by staff, learners, visitors or contractors on College premise regardless of whom owns the equipment. The policy also applies to any equipment, regardless of physical location, which is used by staff or contractors when undertaking their duties.

The College recognises that the distinction between computer use at work and at home is increasingly blurred, with many of us now using our own computers for work. While the College neither wishes nor intends to dictate how you use your own computer, staff should consider that the spirit of this policy applies whenever you are undertaking an activity that stems from your employment with the College.

3 Legislation

- Data Protection Act 1998
- Computer Misuse Act 1990
- Freedom of Information Act 2000
- Copyright Designs & Patents Act 1988
- Malicious Communication Act 1998
- Criminal Justice & Public Order Act 1994
- Telecommunications Act 1984
- Counter-Terrorism and Security Act 2015

4 Responsibilities

Everyone has a responsibility to give full and active support for the policy by ensuring:

- The policy is known, understood and implemented
- Everyone is treated with respect and dignity

- Behaviour not in accord with the policy is challenged.

If a user fails to comply with any legislation or policy, including any of the acceptable use provisions outlined in this document, use of the system may be withdrawn and future access may be restricted. This may impact on the individual's ability to undertake the duties of their job or continue their studies.

Serious or consistent non-compliance with this policy may be considered to be a disciplinary offence and will be dealt with in accordance with the College's Disciplinary procedure or other appropriate action may be considered.

5 Expectations

You must at all times conduct your computer usage professionally, which includes being polite and using the system in a safe, legal and business appropriate manner.

5.1 Acceptable Use

The College computer systems are intended to be used by

- Learners currently enrolled on a course in the support of their studies
- Employees in support of their approved duties
- Contractors in support of work for which they have a current contract with the College.
- Official visitor to the College in support of the purposes of their visit

Usage of the IT Systems may be made for limited and reasonable personal usage, provided this is:

- not associated with monetary reward
- undertaken in the users own time
- not interfering with the delivery of College services
- does not prevent other users from carrying out their studies or assigned duties
- does not violate this or any other College policy
- a lawful activity.

5.2 Unacceptable Use

Among uses that are considered unacceptable are the following:

- Downloading or installing any software, executable files or other potentially harmful material without the express permission of IT Services team.
- Using, transmitting, or seeking inappropriate, offensive, pornographic, vulgar, suggestive, obscene, abusive, harassing, threatening, racist, sexist, or defamatory language or materials;
- Making ethnic, sexual-preference, or gender-related slurs or jokes;
- Encouraging the use of controlled substances;
- Accessing material or propaganda from extremist* organisations and / or using social media to share, comment or promote beliefs and messages of extremist ideologies.

  * Definition of extremist in the context is "vocal or active opposition to fundamental British Values, including democracy, the rule of law, individual liberty and mutual respect and tolerance of different faiths and beliefs. We also include in our definition of extremism calls for death of members of our armed forces"

- You must respect, and not attempt to bypass, security or access restrictions in place on the computer system.

- You must not intentionally damage, disable, or otherwise harm the operation of computers
- Transmitting or making copies of materials protected under copyright law where this action would breach that law.
- Conducting non-approved business
- Conducting unauthorised political activity for personal gain or to promote extremist groups or policies
- Conduct any non-College related fund raising or non-College related public relations activities
- Attempting to impersonate another individual, or fraudulently claiming to represent the interests of any other party
- Transmit images or videos of an individual, or group of individuals, unless it is reasonably believed that consent of the subjects has been obtained.
- Attempt to subvert the course of an ongoing disciplinary procedure.
- Deliberately infect, or attempt to infect, the College systems with a virus or other form of malware.
- Using the system for any other criminal or unlawful purpose, including obtaining unauthorised access to or otherwise interfering with any computer system by 'hacking'.

The College expects users to follow the same standards of behaviour when using privately owned devices on Campus as they would when using College owned equipment. For example, it would not be acceptable to use a privately owned laptop to display obscene images on campus.

Should users indulge in unacceptable use as defined above they will be subject to disciplinary action under the appropriate procedure, in certain cases this may amount to gross misconduct.

5.3 Terrorism

The Terrorism Act (2006) outlaws web posting of material that encourages or endorses terrorist acts, even terrorist acts carried out in the past. Sections of the Terrorism Act also create a risk of prosecution for those who transmit material of this nature, including transmitting this material electronically.

Visits to websites related to jihadism and downloading of material issued by jihadist groups (even from open-access sites) may be subject to monitoring by the police.

6 Security

Access and usage of systems must be in accordance with the College's Information Security Policy.

- You must not reveal your account password or allow another person to use your account
- You must not use another individual's account, nor attempt to log on as another user
- You must notify the IT Helpdesk immediately if you identify a security problem, including out of date virus protection.
- You must not show or identify any security problems you discover to anyone other than the College's IT staff
- You must use only properly supplied and authorised systems for undertaking College business

- You must not attempt to circumvent any security measures or virus protection put in place by IT Services.
- When leaving a computer unattended, you must either log off your account or lock the computer to prevent anyone using your account in your absence.
- You must not store any sensitive or personal information about staff or students on any portable storage system (such as a USB memory stick, portable hard disk, or personal computer) unless that storage system is encrypted and approved for such use by the College.
- If you use a personal computer at home for work purposes, you must ensure that any College-related sensitive or personal information is secured to prohibit access by any non-member of staff, and encrypted to protect against theft.

6.1 Passwords

General guidance:

- Avoid using passwords with obvious personal connections, for example, names of pets, favourite football team, names of your children, nick names, etc…
- Avoid using passwords with obvious work/college related connections passwords, for example, college123, marine, etc…
- Do not use common, or default, passwords, for example, “password1”, “abc123”,”letmein”
- Do not reuse the same password, we recommend using a different password for everything
- Where available use Multi-factor Authentication (MFA)
- Good advice is to pick three random words and use these as your password e.g. “whiteraccoonlime” adding in numbers or special characters as required, “wh1te racoon lime” (“space” is a special character)

Storage of passwords:

- Do not use web browser (Chrome, Internet Explorer etc…) “remember password” features
- Do not store passwords in a password protected Excel, Word, or other document
- If you have to write a password down it should be stored in a sealed envelope and placed in a lockable cupboard, or safe
- If you have a lot of passwords to remember use a password manager application (**College employees must only use password managers that have been approved and procured by IT Services for storage of work related passwords.**)

Password requirements:

- Staff
    - 8 characters long, mix of lower case & upper case letters, numbers and special characters.
    - 30 day expiration
    - 12 most recently used passwords remembered
- Learners
    - 10 characters long
    - No expiration

7 Monitoring & Privacy

All communications and data that are sent, received, created or contained within the College's IT Systems are the property of the College. The College reserves the right to monitor, log and access all computer, telephone and network activity including internet access and e-mail, with or without notice, to or from any device owned by the College, or connected to the College's IT Systems.

Monitoring and access will take place in order to:

- Establish the existence of facts
- Investigate disciplinary issues
- Detect and/or prevent crime
- Ensure that any use (including any personal use permitted by this policy) is lawful and complies with this policy
- Ensure the operational effectiveness of the IT Systems, i.e. protection against malware, spam, etc…

The College may make and keep copies of email and other data stored or transmitted via its systems for any of the above purposes. Users should, therefore, have no expectations of privacy in the use of these systems.

When recording telephone conversations the College will make every effort to inform both parties that recording is taking place. This does not apply to the routing monitoring of telephone activity logs which do not contain recordings of conversations.

E-Mail access will be regularly and actively monitored by the College to ensure usage is in accordance with this policy. In particular monitoring will be undertaken to identify and eliminate any messages which may be harmful to the operation of IT Systems. For example, spam e-mails and e-mails containing malware. Records may also be maintained for evidentiary purposes to satisfy funding body or legislative requirements.

Monitoring of usage and access to systems will be made with the authorisation of the Head of IT or their appointed deputy.

8 E-Mail

E-Mail accounts are provided to all users of the College network. Access to and usage of e-mail must be in accordance with this policy. The College reserves the right to withdraw access to e-mail from any device, or individual, at the discretion of the Head of IT.

Email is not a secure method of communication, and can be easily copied, forwarded and archived. Unless explicitly authorised to do so, you must not send, transmit, or otherwise distribute proprietary information, copyrighted material, trade secrets, or other confidential information belonging to the College.

Use of e-mail for personal purposes is permissible provided this usage is in accordance with this other provisions in this policy.

9 Legal Commitments and E-Mail

E-mail can result in binding contracts. Users should be aware that legal commitments can result from their e-mails. The same degree of care should be exercised as with any other written communication.

For evidential purposes, it is the responsibility of the individual who sends, or receives, the e-mail that a suitable record of any messages which evidence commitments is made.

Personal e-mail accounts, for example, Hotmail, Yahoo, Googlemail etc should not be used for official communications.

10 Additional Regulations

All Users must comply with the additional regulations that relate to the use of particular aspects of the IT facilities. This includes the following documents:

Joint Academic Network (JANET) Acceptable Use Policy available from:
https://community.jisc.ac.uk/library/acceptable-use-policy

11 Related Policies

- Harassment and Bullying Policy
- Data Protection Policy
- Information Security Policy
- E-Safety Policy
- Control of IT Software and Hardware Policy
- Staff Disciplinary Procedure and Policy
- Social Media Policy
- Copyright Policy