Remote Working Policy

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: Director of IT
- 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.

Approved by:	Version:	Issue Date:	Review Date:	Contact Person:
Exec Group, JCC	V2	April 2024	April 2027	Director of IT

Review: **3 years**

Policy Number 103

Remote Working Policy

1. Policy Statement

Remote or mobile working involves access to College systems from outside of our on-premises infrastructure. This brings about great benefits to the College in terms of flexibility and efficiency, but also exposes it to risks that must be managed.

This policy supports our aim to allow staff and students to work from any location, using any suitable device whilst ensuing the confidentiality, integrity and availability of the College's data and systems.

2. Scope

- This policy applies to all members of the College community (staff (including agency workers), governors, students, and contractors/suppliers.

- This policy covers all College data and systems being accessed electronically from remote locations or via mobile devices.

- For the purposes of this policy, the terms "mobile" and "remote" are used interchangeably, and should be taken to cover any scenario where College data or systems are accessed from off campus.

3. Legislation

- Computer Misuse Act 1990
- Data Protection Act 2018
- General Data Protection Regulation 2018

4. Responsibilities

4.1. The Director of IT is responsible for ensuring all staff are aware of the policy and the need to adhere to it when working remotely.

4.2. All staff are responsible for adhering to the policy.

4.3. Where the policy requirements are reliant upon individual staff taking steps to secure any data they are handling they may be held personally accountable for failing to follow the required policy, procedure or process.

5. Authorisation for Remote Access

5.1. Remote access is available for use by all staff and students

5.2. Multi-factor authentication (MFA) is required for all remote access by staff, and for student access to remote desktop facilities.

5.2.1. Staff who have chosen to opt out of MFA will not be permitted to access any systems remotely

5.2.2. Students who have not provided the college with a mobile phone number will not be able to access remote desktop facilities

5.3. Complete or partial remote access may be revoked from any individual where:

- we have reason to believe the facilities are not being used for purposes for which they are intended.
- we believe their account may have been compromised;
- or, we believe they are not abiding by this policy.

6. Available resources

6.1. Direct access over the internet will only be provided to systems that are designed and intended to be published on the public internet (for example, outlook web access, Teams, Moodle etc…)

6.2. Access via remote desktop facilities will be provided for other applications where:

- there is a business need to access the software remotely;
- applicable software licence agreements allow use of the software in this manner;
- the software manufacturer supports its use in a remote desktop/virtual desktop platform

6.3. Remote desktop client "pass though" features that substantially increase the risk of malware infection, data theft and data loss will be disabled. This includes, but is not limited to, printers, local drives, and USB devices.

7. General principals

7.1. Staff should not access or work on tasks involving personal, confidential, or highly confidential data in public locations.

7.2. Staff should ensure that the environment in which they are working in offers a suitable level of privacy for the task in hand (e.g. other individuals in the vicinity being able to view papers, or screens, or being able to overhear private conversations)

7.3. Staff should never leave papers or equipment containing personal, confidential, or highly confidential data unattended unless they are appropriately physically secured from theft.

7.4. Public or free wi-fi services should not be used for remote working. Free wi-fi services provided in cafes, hotels and other establishments can easily be impersonated by cyber-criminals. This technique is being increasingly used to steal data and credentials

8. Use of personal equipment

8.1. Use of personally owned mobile phones may be used for work purposes both on-campus (BYOD) and off-campuses

8.2. Staff use of personally owed laptops or desktops is not permitted

8.3. Staff have a responsibility to ensure that when using personally owned equipment they:

- install the latest patches/updates within 14 days of release;
- password protect the device;
- only use approved software and collaboration tools. Before downloading any software or tools for work purposes, check that they are approved by IT Services;
- only download apps for mobile phones and tablets from manufacturer-approved stores like Google Play or the Apple App Store;
- do not use any jailbroken devices or 'rooted' Android devices for work;
- make sure they are running antivirus software on any personal desktops or laptops they are using;
- enable any firewalls that are present on the devices;
- and if working from home
    - enable password protection on their home Wi-Fi, if it isn't set up already
    - Change the default password on their home wi-fi & router, if they haven't done so already.

9. Related Policies

- Information Security Policy
- Acceptable use of ICT Policy
- Data Protection Policy