ICT ACCEPTABLE USE POLICY

College Policy No	**IT01**
Approved by	**Vice Principal - Corporate Services**
Original Issue Date	**17/04/2017**
Current Issue Date	**20/01/2023**
Review Date	**23/10/2023**

CONTENTS

1 PURPOSE

The guiding philosophy of this policy is that the College's ICT facilities should be used in a manner which is ethical, legal, appropriate to the College's aims, and not to the detriment of others.

This policy is designed to protect users and the College from the negative impact caused by the inappropriate use of ICT facilities. It does this by:

- Outlining the principles applicable to the use of ICT facilities and the ownership of data.
- Identifying the processes used to authorise, control and manage the creation of staff, student and third-party user accounts which give access to College ICT systems.
- Giving examples of acceptable and unacceptable use.
- Supplying clear and consistent guidance for all users.

This policy should not be read in isolation. College ICT systems, networks and equipment allow users to connect to third party services over the UK Joint Academic Network (Janet) and/or the internet. By using the College facilities users are agreeing with the acceptable use policies of the services that they use as well as the policies and legislation referenced in this document.

2 SCOPE

This policy covers the use of all College ICT encompassing systems, networks, and equipment whether on-site or off-site. This includes, but is not limited to, the use of College data and the accessing of third-party data and systems via the College network. This policy applies to all staff and students of the College and any other person authorised to use these facilities (hereafter referred to as 'users').

For the avoidance of doubt, this policy applies to users utilising their own ICT equipment to access College data and systems and/or to connect to the College network.

In this policy systems, networks and equipment includes services such as those provided by ICT or by any other department of the College. This includes any ICT services delivered for the College via an external partner.

3 GENERAL USE OF ICT AND OWNERSHIP OF DATA

College ICT facilities are maintained for the sole purpose of supporting the teaching, learning, research, and business activities of the College. They may be used for any legal activity that furthers the aims and objectives of the College.

To use the College ICT facilities users must agree to abide by this policy and adhere to College policies and legislation related to Copyright, Information Security and Computer (mis)use.

ICT facilities may be used for limited personal use, so long as that use is not at odds with the underlying philosophy of this policy and does not in any way interfere with the aims and purposes of the College. Such limited personal use must not include use for commercial purposes.

The data held on College ICT facilities may be proprietary and/or confidential in nature. Users should only access data that they are authorised to access. Any processing of data should be done so following the College Data Protection Policy. All data held will be fall under the Freedom of Information Act.

Proprietary and/or confidential information or software owned or licensed by the College should not be copied and/or removed from College systems without prior written authorisation from the College Data Protection Officer and the Head of ICT Services. When the copying of College data to third party equipment, systems or storage devices is authorised, this should be done following the Data Protection Act, the College Data Protection Policy, and the terms of any software licensing agreements. It should be noted that the ownership of the copied data remains with the College regardless of the ownership of the device or system that it is transferred to.

As outlined in the Data Protection Policy, users are reminded of their responsibility to promptly report the theft, loss, or unauthorised disclosure of proprietary and/or confidential information owned by the College. Staff and students can report incidents directly to the College Data Protection Officer, ICT Helpdesk or to a line manager. Additionally, students can also report incidents to the ICT Helpdesk, Student Services, or any member of Curriculum Staff.

For security and management purposes, authorised users may monitor facilities usage at any time without warning. The College reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

4 ACCESS AND ACCOUNT TYPES

Access to College ICT facilities is authorised by the allocation of a unique user identifier (username) and a password.

As a guide, access to ICT facilities will be role-based rather than person-based. For example, if a device or access is required by an employee to enable them to complete their role and they then move to a different role then access to the device/system will be revoked.

Four types of accounts are used to provide access to College ICT facilities

4.1 Staff Accounts

Staff accounts are created and assigned to users employed by the College.

The assignment of staff accounts is an automated process which is linked to the People Team recruitment process. Staff user accounts are created shortly prior to a new member of staff joining the College and are automatically disabled and archived when a user's employment ends.

Staff accounts may have access to student facing and administrative systems within the College. The exact nature of access is dependent on the role of the user and the team in which they work.

4.2 Student Accounts

Student accounts are accounts created and assigned to users who attend the College as a student.

The assignment of student accounts is an automated process which is linked to the Academic recruitment process. Student user accounts are created as part of the enrolment process and are automatically disabled and archived when a student completes their course of study.

Student accounts only have access to student facing systems within the College.

4.3 **Third Party Accounts**

Third party accounts are accounts created and assigned to users required to access College ICT facilities who have a relationship with the College but are neither a staff member nor a student. Examples of this include:

- Care workers employed by the local authority to support a student through their studies
- Guests and visitors invited to work in or with the College by an existing member of staff
- Commercial organisations required to carry out development or support

The assignment of third-party accounts is a manual process which can be instigated by any member of staff. Third party accounts are linked to the staff member who requested the account to ensure that it is always possible to show who requested the account. Third party accounts are created for a defined period, after which they are automatically disabled and archived.

Third party accounts may have access to student facing and administrative systems within the College.

4.4 **Administrator Accounts**

In a small number of cases (mainly within ICT Services, but any member of staff can request one) an administrator account can be created which is assigned to individuals. These are accounts to be utilised when a user is required to have temporary raised privileges on the college network.

All administrator account requests, and specific access required are approved by the Head of ICT. Decisions on granting an administrator access will be based on :-

- The type of elevated access required
- The requestors job specification
- Approval from a line manger
- Whether there are alternatives to not creating an administrator account to the user
- The ability to grant appropriate additional access without providing an administrator account that has excessive access to systems.

The administrator accounts cannot be used to log into a device but utilised to elevate access at an appropriate time to complete a specific process.

The administrator account should only ever be used to complete the task that the account was provisioned for which will be outlined on the issuing of the account. If the account is used for anything other than what it was intended this will be deemed a contravention of this policy and would be dealt with through the College disciplinary process.

5 APPROVED SOFTWARE

College corporate devices will be provisioned with the most used software. If additional software is required, then the primary user of that device is able to select the software required from a list of pre-

approved applications. The list of pre-approved applications and the functionality to install these can be found in the Company Portal application, which can be found on all corporate devices.

If a user requires to have additional software installed on their corporate device, which isn't in the approved software inventory list, then this can be requested through the ICT Helpdesk.

6 ROLES AND RESPONSIBILITIES

All users are expected to exercise good judgement and to act in a manner that does not cause damage to College ICT facilities. Any damage must be reported to the ICT Helpdesk at the earliest opportunity. Any malicious damage could result in disciplinary action and/or criminal prosecution.

6.1 Account Security

Users are not allowed to use another user's accounts to access College ICT facilities and should not allow others to access their user id and password. The individual to whom a user id is assigned will be held responsible for all activity initiated by and/or undertaken using that user id.

If a user suspects that someone else has gained access to their account, they should report this to the ICT Helpdesk and change their password using the Office 365 service (https://www.office.com) at the earliest opportunity.

6.2 Password Security

Users should choose a password which is secure and not easily guessed. For security reasons, passwords should not be printed or shared with others.

The network password will expire after 365 days and must be changed prior to the 365th day to ensure continued access to ICT facilities.

6.3 Sharing Information

Users are reminded of the need to exercise caution when sharing personal information about themselves and others in public forums such as social media. Users should limit the amount of personal information that they make public and should be wary about sharing personal information with social media contacts.

6.4 Acceptable Use

College ICT facilities are maintained for the sole purpose of supporting the teaching, learning, research, and business activities of the College.

College ICT facilities may be used for any legal activity that furthers the aims and objectives of the College.

Limited personal use of College ICT facilities may be justified so long as it does not interfere with the operation of the College or the furtherance of its aims and objectives. Such limited personal use must not include use for commercial purposes.

6.5 Unacceptable Use

Examples of unacceptable use of College ICT facilities are listed below. This list is not exhaustive and should be considered as guidance only.

When using College ICT facilities users must not:

- Participate in activities which may bring the College into disrepute
- Participate in activities which could result in civil or criminal action being taken against the College, its staff or students

- Participate in activities which promote or support terrorism or which promote or support extremist views and/or activities
- Store, create, display, or propagate material which falls into any of the following categories:
  - Grossly offensive
  - Indecent
  - Menacing in nature
  - Intended to misinform and thereby cause annoyance, inconvenience, or needless anxiety to others
  - Illegal or prohibited by legislation
  - Infringement of copyright
- Attempt to gain unauthorised access to ICT facilities
- Deliberately store, create or propagate viruses, spyware, ransomware, or other malicious software
- Use another user's account for any purpose
- Undertake unauthorised monitoring of network communications
- Read any other user's email without permission and authorisation
- Participate in behaviour which would be considered clearly unacceptable by others. Examples of behaviour which would be considered clearly unacceptable includes, but is not limited to:
  - Online stalking
  - Grooming
  - Soliciting of children or vulnerable people
  - Defamation
  - Creation of distribution of offensive material
  - Fraud
  - Software/copyright theft
  - Intentional damage to College equipment, systems, networks, or data
  - Unauthorised retention of other people's personal information
  - Drug related activities

7 BREACH OF POLICY

Any breach of this policy will be subject to investigation in line with the College Staff Discipline Policy and Student Code of Conduct.

Users found to have engaged in unacceptable use of College ICT systems and networks will be considered to have misused ICT facilities. The misuse of ICT facilities is regarded as a disciplinary matter.

Disciplinary action up to and including dismissal may be taken against any member of staff who has been found to have misused College ICT systems and networks.

Disciplinary action as outlined in the Student Code of Conduct may be taken against any student who has been found to have misused College ICT systems and networks.

Where civil or criminal law appears to have been breached, the College may refer the case to Police Scotland.

8 DEFINITIONS

COMPUTER VIRUS: A computer virus is a type of computer program that, when executed, replicates itself by changing other computer programs and inserting its own code.

ICT FACILITIES: Encompassing ICT Systems, Networks and Equipment.

ON-SITE / OFF-SITE: On-Site is any activity which happens on the College campuses. Off-site is activity anywhere else e.g. Schools, Home, Public

NETWORK ACCOUNTS: Profile held on the college network to allow users to connect to the network and ICT to track individual use

RANSOMWARE: A type of application that threatens to publish the victim's data or perpetually block access to it unless a ransom is paid.

SOCIAL MEDIA: Online services for communicating and sharing of personal information

SPYWARE: Software that aims to gather information about a person or organization, sometimes without their knowledge, and send such information to another entity without the consumer's consent.

UNAUTHORISED ACCESS: Accessing a resource without permission from relevant system owner

9 REFERENCES

Bring Your Own Device Policy
Client Device Policy
Computer Misuse Act 1990
Copyright, Designs & Patents Act 1998
Copyright Policy
Data Protection Act 2018
Data Protection Policy
Data Protection Process
Freedom of Information (Scotland) Act 2002
Information Security Policy
Janet Acceptable Use Policy
Janet Security Policy
Malicious Communications Act 1998
Mobile Device Process
Record Management and Data Retention Policy
Staff Disciplinary Policy
Staff Discipline Process
Staff Social Media Policy
Student Code of Conduct
Student Electronic Communication Policy