ICT ACCEPTABLE USE POLICY

Strategic Aim	To continue to develop and ensure effective leadership, governance and management throughout the organisation
Responsibility	Vice Principal, Business Development and Corporate Services
Issue Date	27/05/2020

Equality Impact Assessment	27/05/2020

Introduction

There needs to be commitment to protect Dumfries and Galloway College employees, students, Academic Partners and the wider Joint Academic Network (JANET) organisation from illegal or damaging action by individuals, either knowingly or unknowingly.

As a user of 'computer services' of Dumfries and Galloway College you have a right to use its 'computing services'; that right places responsibilities on you as a user which are outlined below. Inappropriate use exposes Dumfries and Galloway College to risks including virus attacks, compromise of network systems and services, and legal issues.

If you misuse the 'computing facilities' in a way that constitutes a breach or disregard of the following policy you may also be in breach of other College policies.

Ignorance of this policy (or those that it directs you to), and the responsibilities it places on you, is not an excuse in any situation where it is assessed that you have breached the policy and its requirements.

Students and staff who connect their own devices to the College's network and the services available are particularly reminded that such use requires compliance to this policy.

Students are directed to this policy during their enrolment each year and are required to acknowledge their agreed adherence to and compliance with the policy each time they log on to the network.

Staff are advised of this policy during their induction and of the College's requirement for them to adhere to the conditions therein.

1 Purpose

The purpose of this policy is to outline the acceptable and unacceptable use of 'computer services' owned by Dumfries and Galloway College.

2 Scope

This policy applies to employees, Board of Management, students, contractors, consultants, temporaries, and other workers at Dumfries and Galloway College, including all personnel affiliated with third parties. This policy applies to all equipment that is owned or leased by Dumfries and Galloway College and to all equipment connected to the College's network. Use of Dumfries and Galloway College ICT equipment and the Dumfries and Galloway College network are limited to staff, students and authorised third parties only. Under no circumstances should any person not included in the above list be allowed to access to the Dumfries and Galloway College network.

3 Disciplinary Procedures

3.1 Staff or students who contravene this policy may find themselves subject to the College's disciplinary procedures.

3.2 Individuals may also be subject to criminal proceedings. The College reserves its right to take legal action against individuals who cause it to be involved in legal proceedings as a result of their violation of licensing agreements and/or other contraventions of this policy.

4 Definitions

4.1 For the purposes of this policy the term "computing services" refers to any IT resource made available to you, any of the network borne services and the network/data transport infrastructure that you use to access any of the services. Including services provisioned and accessible (both wired and wireless) through individual accounts and passwords. Such services would include access to internet/ intranet related systems, including but not limited to computer equipment, software, applications, databases, operating systems, storage media, network accounts, cloud based storage, email accounts, internet browsing, and FTP and are the property of Dumfries and Galloway College. These systems are to be used for educational purposes in serving the interests of the organisation, and of our staff and students in the course of normal operations.

4.2 The term "**devices**" includes but is not restricted to: laptops, tablets, smart phones and any Wi-Fi connected device

4.3 Definitions of Unacceptable Usage
Unacceptable use of College computing services may be summarised as, but not restricted to:

- Actions which cause physical damage to any ICT hardware, including peripherals (eg, mouse, keyboards, cables, wiring, printers);
- Creating, displaying or transmitting material that is fraudulent or otherwise unlawful, likely to cause offence or inappropriate;
- Threatening, bullying, intimidating or harassing staff, students or others;
- Intellectual property rights infringement, including copyright, trademark, patent, design and moral rights;
- Defamation;
- Unsolicited advertising, often referred to as "spamming";
- Sending emails that purport to come from an individual other than the person actually sending the message using, eg, a forged address;
- Attempts to use any ‘computing services’ for the purposes of bribery;
- Attempts to break into or damage computer systems or data held thereon;
- Actions or inactions which intentionally, or unintentionally, aid the distribution of computer viruses or other malicious software, eg use of equipment which is inadequately protected against viruses and spyware;
- Attempts to access or actions intended to facilitate access to computers for which the individual is not authorised;
- Using the College network for unauthenticated access;

- Unauthorised resale of College, or JANET services or information;
- Using the ‘computing services’ for gambling;
- Using the ‘computing services’ for carrying out any illegal trading activity; and
- Any other conduct which may discredit or harm the College, its staff or the College ‘computing services’;

These restrictions should be taken to mean, for example, that the following activities will normally be considered to be a breach of this policy:

- The use of peer-to-peer and related applications within the College;
- Interfering with data or settings in another person’s network account;
- Users must not deliberately visit, view, download, print, copy, forward or otherwise transmit any unlawful material or that which is likely to cause offence;
- The downloading, distribution, or storage of music, video, film, or other material, for which you do not hold a valid licence, or other valid permission from the copyright holder;
- The distribution or storage by any means of pirated software;
- Connecting an unauthorised device to the College network, ie one that has not been configured to comply with this policy and any other relevant regulations and guidelines relating to security, purchasing policy, and acceptable use;
- Circumvention of network access control;
- Monitoring or interception of network traffic, without permission;
- Probing for the security weaknesses of systems by methods such as port-scanning, without permission;
- Associating any device to network Access Points, including wireless, to which you are not authorised;
- Non-academic activities which generate heavy network traffic, especially those which interfere with others' legitimate use of ‘computing services’ or which incur financial costs;
- Excessive use of resources such as file store, leading to a denial of service to others, especially when compounded by not responding to requests for action;
- The use of College mailing lists for non-College business;
- The use of portable media for the purpose of copying unlicensed copyright software, music, etc.

If you mistakenly access such material you should notify the ICT Department. You should be aware that you will be held responsible for any claims brought against the College.

In the event of any use that could be regarded as giving rise to criminal proceedings the College may inform the police or other law enforcement agency. Other uses may be unacceptable in certain circumstances.

5 Key Principles

5.1 Authorisation

In order to use the ‘computing services’ of the College a person must first be properly registered to use such services. Registration to use the College ‘computing services’

implies, and is conditional upon acceptance of this Acceptable Use Policy as part of the College regulations, by agreeing to the Terms and Conditions of enrolment. The lack of a signature does not exempt an individual from any obligation under this policy. The continuing use of the ICT Facilities will be deemed to be acceptance by the user of the terms of this policy.

The enrolment procedure grants authorisation to use the core 'computing services' of the College relevant to your post. Following enrolment, a username and password will be allocated to each individual user. Authorisation for other services may be requested by application to the Dumfries and Galloway College ICT Helpdesk.

Any attempt to access, use or interfere with any user account or email address for which the user is not authorised, is prohibited and will be regarded as a disciplinary offence.

No one may use, or attempt to use, 'computing services' allocated to another person, except when explicitly authorised.

Commercial work for outside bodies involving the use of ICT systems requires explicit permission from the Vice Principal; such use may be liable to charge.

The College recognises that individuals may conduct personal use of email and the Internet. However this must be kept to a reasonable level and must be legal and observe the college expected code of conduct. The College reserves the right to revoke such permission if, in the judgement of the College, these facilities are abused.

5.2 Passwords

A user must take all reasonable precautions to protect the College's resources (including the ICT Facilities and the College's information and data), their username and passwords. Initial passwords should be reset on first use and must register as "strong" at the following site:
https://www.microsoft.com/en-gb/security/pc-security/password-checker.aspx

5.3 Purpose of Use

The College 'computing services' are provided primarily to facilitate a person's essential work as an employee or student or other role within the College. Use for other purposes, such as personal email or recreational use of the Internet, is a privilege which can be withdrawn at any time and without notice. Any such use must not interfere with the user's duties or studies or any other person's use of computer systems and must not, in any way, bring the College into disrepute.

Staff ICT Accounts have been allocated for use by the member of staff in connection with their job requirements. Student ICT Accounts have been allocated for exclusive use by the student in connection with their education whilst at the College.

5.4 Email

College email addresses and associated College email systems must be used for all official College business, in order to support audit purposes and institutional record

keeping. All staff and students of the College must regularly read their College email and delete unwanted or unnecessary emails at regular intervals. Guidance on acceptable email use can be found in the email guidelines in the quality manual on AdminNet.

5.5 **Social media (including e-safety)**

The College recognises the role that social networking and other communication technologies holds within modern student life and learning and teaching practice. The College will use social media in curriculum delivery – particularly in terms of communications with students, gaining feedback, and group discussion; and, for corporate communication, marketing and promotion and for contact with the business community. Facebook and Twitter sites used for corporate communication, marketing and promotion will be managed by the Marketing Team. All staff members using social networking sites as tools through which to communicate with students must only do so on a professional basis. Guidance on use of social media and in particular, e-safety' can be found in the social medial guidelines in the quality manual on AdminNet and LearnNet.

5.6 **Copyright Compliance**

Employees and students must not download, copy or otherwise re-produce material for which they have not obtained permission from the relevant copyright owner. If such material is required for any purpose eg teaching or research then copyright permission must be obtained and documented before such material is used.
Employees and students are reminded that the College treats plagiarism very seriously and will investigate any allegation ie the intentional use of other people's material without attribution.

5.7 **Data Protection**

All users must adhere to the College's Data Protection policy and procedures.

5.8 **Privacy and Monitoring**

All allocated usernames, passwords and email addresses are for the exclusive use of the individual to whom they are allocated. The user is personally responsible and accountable for all activities carried out under their username. The password associated with a particular personal username must not be divulged to any other person. Passwords should not be recorded where they may be easily obtained and should be changed immediately if it is suspected that they have become known to another person.

The College reserves the right for appropriately authorised staff to examine any data including personal data held on College systems or, when operationally necessary, for example to give access to a private account to a line manager or colleague. Certain staff within the College have been authorised to examine files, emails and data within individual accounts, but will only do so when operationally necessary.

It is also occasionally necessary to intercept network traffic. In such circumstances appropriately authorised persons will take all reasonable steps to ensure the privacy of service users. Logs will be kept of usage of IT equipment; this will include dates and times when accounts were accessed.

The College reserves the right to monitor email, telephone and any other electronically mediated communications, whether stored or in transit, in line with the Regulation of Investigatory Powers Act (2000) and other relevant law.

Reasons for such monitoring include the need to:

- Establish the existence of facts (eg to provide evidence of commercial transactions in cases of disputes);
- Investigate or detect unauthorised use of the College's telecommunications systems and ensure compliance with this policy or other College policies;
- Ensure operational effectiveness of services (eg to detect viruses or other threats to the systems);
- Prevent a breach of the law or investigate a suspected breach of the law, the College's policies and contracts;

When a student or member of staff leaves the College (either on completion of course or termination of employment, files left on any computer system owned by the College, including email files, may be removed. The College is under no obligation to recover any data once a person has left the College. Before leaving the College, staff should make arrangements with their Manager to transfer to colleagues any relevant email or other computer-based information held under their personal account.

When a member of staff is away it may be necessary for appropriately authorised members of staff to access the absent member of staff's email account and network files to deal with matters in their absence. This should be borne in mind when using the 'computing services' for personal reasons. Users should consider adopting appropriate markers for personal and private emails.

For operational reasons and for the continuing delivery of services, the College has the right to access the personal account of a staff member after that person leaves.

Users of 'computing services' should be aware that the College conducts random monitoring of communications, regardless of whether the use is business or personal.

Where abuse is suspected (especially criminal activity and/or gross misconduct), the College may conduct a more detailed investigation involving further monitoring and examination of stored data (including employee-deleted data) held on servers/disks/drives or other historical/archived data.

Where disclosure of information is requested by the police (or another law enforcement authority) the request where possible will be handled by the College's Data Protection Officer or other appropriate senior person.

The College is committed to achieving an environment which provides equality of opportunity, and freedom from discrimination. Distributing material, which is offensive, obscene or abusive, may be illegal and may also contravene College codes on harassment. No carrying out of unauthorised surveillance, audio and/or visual, of a student, staff or member of the public on Dumfries and Galloway College premises is permitted.

No user shall interfere or attempt to interfere in any way with information belonging to or material prepared by another user. Similarly no user shall make unauthorised copies of information belonging to another user. The same conventions of privacy apply to electronically held information as to that held on traditional media such as paper.

All users will abide by laws relating to the use and protection of copyright.

Users of services external to the College are expected to abide by any policies, rules and codes of conduct applying to such services. Any breach of such policies, rules and codes of conduct may be regarded as a breach of this Acceptable Use Policy and be dealt with accordingly. The use of College credentials to gain unauthorised access to the facilities of any other organisation is similarly prohibited.

6 Responsibilities

6.1 The responsibility for the supervision of the Acceptable Use Policy is delegated to the ICT Manager. Any suspected breach of this policy should be reported to a member of ICT Support staff. The Vice Principal will then take the appropriate action. Actions will include, where relevant, immediate removal from online information systems of material that is believed to infringe the law. The College reserves the right to audit and / or suspend without notice any account pending any enquiry. Where necessary, this will include the right to intercept communications.

6.2 This policy is not exhaustive and inevitably new social and technical developments will lead to further uses, which are not fully covered here at present. In the first instance students should address questions concerning what is acceptable to their personal tutor. Staff should approach their line manager. Where there is any doubt the matter should be raised on a TSR with ICT Department, whose staff will ensure that all questions are dealt with at the appropriate level within the College.

7 Linked Policies/Related Documents:

Registration for Computing Services for Student Use
Registration for Computing Services for Staff Use
Data Protection Policy and Guidelines
ICT Security Policy
Safeguarding Children, Young People, Adults at risk Policy and Procedure
Disciplinary Procedure (Staff)
Student Disciplinary Procedure
Code of Conduct Policy
Anti Bullying Policy
Marketing Policy

8 Relevant Legislation:

Copyright, Designs and Patents Act 1988
Malicious Communications Act 1988

Computer Misuse Act 1990
Trade Marks Act 1994
Data Protection Act 2003
Human Rights Act 1998
Regulation of Investigatory Powers Act 2000
Freedom of Information (Scotland) Act 2002
The Bribery Act 2010

DISTRIBUTION LIST
All Staff
LearnNet
Quality Manual