Dumfries and Galloway College
One step ahead

# ICT ACCEPTABLE USE POLICY

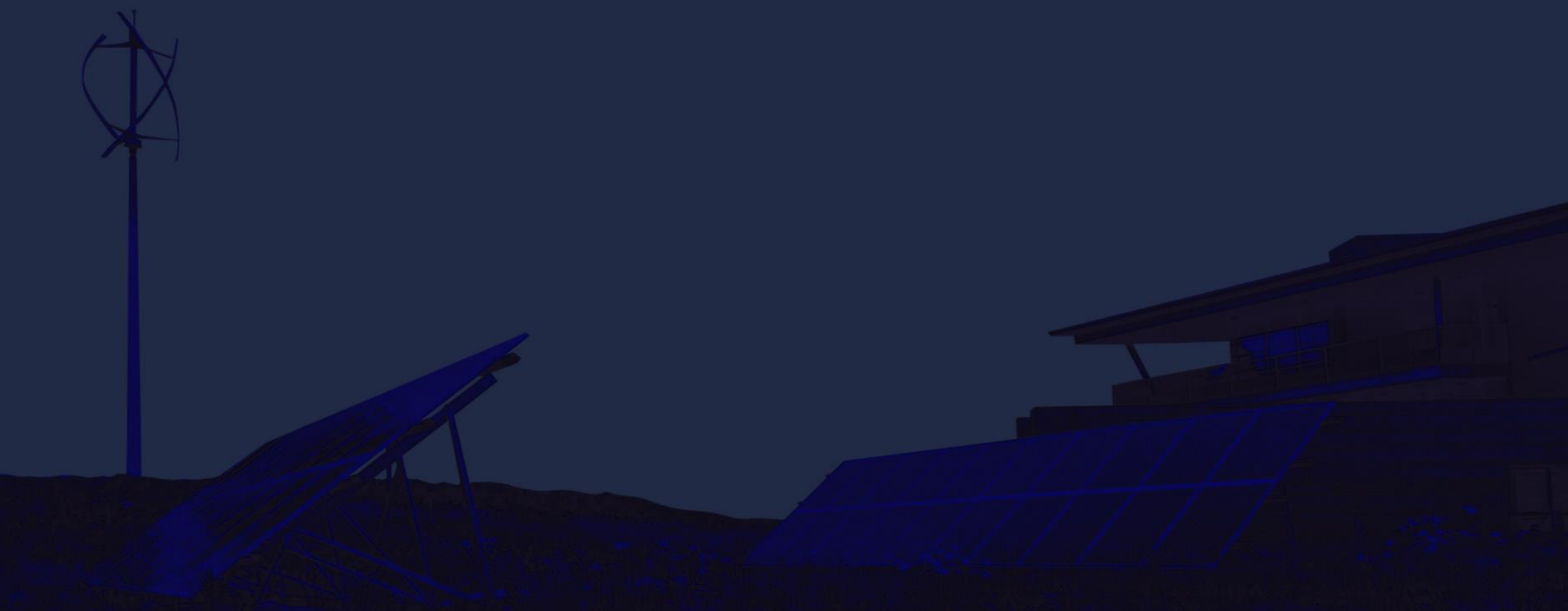
**Responsibility: Vice Principal, People and Transformation**

**Issue Date: 31st August 2023**

**Equality Impact Assessment: 28.08.23**

---

Version: 1



## Table of Contents

# ICT Acceptable Use Policy

## *1. Purpose*

The policy is intended to protect users and their data, and the College from illegal or damaging actions by individuals, either knowingly or unknowingly. 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.

Inappropriate use by individuals will be managed in accordance with College policies and procedures, including the Disciplinary Policy and the Code of Student Behaviour.

It will also be reported to law enforcement agencies if appropriate.

The aim of the Dumfries and Galloway College Acceptable Use Policy (AUP) is to reflect the established culture of openness, trust, and integrity.

The purpose of this policy is to outline the acceptable (and prohibited) use of college computer equipment and network access. Inappropriate use exposes the College to a range of risks including virus attacks, compromise of network systems and services, and legal issues. This policy also prohibits accessing College ICT facilities to cause harm or offense to others.

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.

All internet access originating from the College network is subject to the JANET Acceptable Use Policy: https://community.jisc.ac.uk/library/acceptable-use-policy.

## 2. *Scope*

This policy applies to all users including staff, students, Board of Management, 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.

Students and staff who connect their own devices to the College's network and the services available require compliance to this policy.

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.

## 3. *References*

This policy is aligned with other policies and procedures within the College, namely:

- Data Protection Policy
- ICT Security Policy
- Learner Behaviour Policy
- Equality and Diversity Policy
- Data Breach Procedure
- Student Disciplinary Procedure

## 4. *Definitions*

- AUP – Acceptable Use Policy
- ICT – Information & Communication Technology
- Spoofing – pertaining to be from another user
- Proxy/Proxies – system that facilitates data exchange between networks
- VPN – Virtual Private Network
- VLE – Virtual Learning Environment (LearnNet)
- MFA – Multi Factor Authentication
- PII - Personally Identifiable Information

## 5. *Responsibility*

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 Digital Services staff. The Vice Principal, People and Transformation 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.

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 the Digital Services Helpdesk, who will ensure that all questions are dealt with at the appropriate level within the College.

## *6. Policy*

### 6.1 Disciplinary Procedures

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

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.

### 6.2 Authorisation and Conditions of Use

#### 6.2.1 Authorisation

Users are provided access to the College ICT Systems when they meet the following categories:

- Members of staff.
- Students.
- Partners of the College (i.e., learning network staff, individuals on work experience, contractors, auditors etc.)

Access will not be restricted on the grounds of disability, impairment or any other protected characteristic.

By logging on to a College system, whether on premise or remotely, users are confirming acceptance of this policy by either clicking accept or ticking an acceptance button prior to logon.

When staff employment or a course of study finishes, access to ICT resources will be revoked automatically and the user accounts will be closed as per internal procedures.

6.2.2 Conditions of Use

ICT resources and Information Systems are provided primarily to support College business such as teaching, training, study, and administrative support of these activities. However, reasonable personal use is also permitted provided there is compliance with this policy. Individuals should exercise due care and attention whilst using College ICT resources to ensure that the corporate reputation remains a priority and no inflammatory posts could be attributed to the College on either internal or external information systems or social media.

Users must not masquerade as someone else and should always keep their logon identity and password private (exceptions will be made for users who have additional support needs). Users should choose a hard to guess password, of which guidance can be found within the College password change procedure which is available from the intranet.

Each user has a personal duty to follow the AUP as diligently as possible, in most cases the College will prefer to inform users of a contravention to the AUP informally while advising corrective action. However, repeated or a serious breach to the AUP will trigger disciplinary procedures.

The following acts can be construed as a misuse and a breach of the AUP:

- Installing software that is not explicitly permitted by the ICT Department.
- The printing, displaying, storing, internet browsing or transmitting of unacceptable or offensive material. This will include material which is:
  - Racially, religiously, sexually, or politically offensive.
  - Obscene, indecent, or pornographic.
  - Likely to promote terrorism or violence.
- The creation or transmission of material which is intentionally designed or likely to cause annoyance, inconvenience, intimidation, or anxiety. This includes cyber- bullying or harassment in any form. Users should ensure that appropriate language and tone should be used in communications at all times in line with College policies and procedures.
- Intentionally affecting security systems or the disruption of network communications, including:
  - Intentionally clicking on known malicious links or running malicious software.

- Implementing a Denial-of-Service attack.
- Excessive or inappropriate use of College network bandwidth.
- Port scanning or information gathering (reconnaissance activity) of network systems exercises.
- Network monitoring/sniffing.
- Providing information about users outwith the College.
- An attack that intentionally disrupts, prevents and/or removes access to computing services within the College or any external organisation.
- Circumventing user authentication or security of any host, network, or account.

- Unauthorised copying, including downloading from the internet, of copyrighted material including, but not limited to, digitisation of photographs from magazines, books, music, applications, or other copyrighted sources.
- Utilising 'proxies' or VPN services to circumvent the College security systems.
- Using computer resources to commit fraud, deception, or another criminal act.
- Vandalism of deliberate physical damage to College equipment.
- Accessing another user's account.
- Impersonating another user whether real (via the user account) or artificial (spoofing). For example, sending messages that appear to originate from another person.
- Sending chain or bulk ('spam') messages.
- Use of College systems for commercial gain, running a business, non-College related advertising, crypto mining, or political lobbying.
- Using unauthorised or unlicensed applications including games, screensavers, drivers, browsers, and plug-ins.
- Adding hardware devices to the College network without explicit authorisation from the Digital Services Department.
- Introducing viruses or malware (e.g., viruses, worms, Trojan horses) designed to impact systems performance, integrity, security, availability to harvest data.
- Breaching or attempting to breach security controls including:
  - Interfering with or disabling anti-virus software.
  - Attempting to change 'safe search' settings.
  - Disabling Windows/Mac update services.
  - Encrypting key College data/systems without authorisation.

- Changing system policies which reduces security (firewalls, modifying logs, disabling encryption on managed devices, etc).

- Any action, or lack of action, which may interfere with the security of College systems or a data breach of Personally Identifiable Information (PII) or sensitive data as per the Data Protection Act 2018 and the General Data Protection Regulations (GDPR).
- Exporting, processing, or transfer of other users' PII or sensitive data outside of secure College systems.
- Contravening the JANET AUP (as referenced on page 3).

It is important that any personal data breaches, or indeed suspected breaches, across the College are reported as soon as possible to the Vice Principal People and Transformation and the Data Protection Officer College as per the Data Breach procedure.

Under the terms of the Data Protection legislation, data controllers have no longer than 72 hours to report a breach to the Information Commissioner's Office after having become aware of it. The College will abide by this statutory requirement.

6.3 Accessing Services or Data Remotely (including on-campus mobile devices)

The College provides several services (email, files, VLE, intranet, etc.) which can be accessed remotely or via guest Wi-Fi services such as Eduroam.

It should be noted that the Internet Protocol (IP), MAC address and browser version data may be recorded when using these systems. This means that location and device browser information can be harvested.

The following requirements shall also apply to user remotely accessing services and data:

**Applies to all users:**

- Users shall only access any remote services using a device that continues to receive security updates from the vendor and ensure that security patches are applied within 14 days of release.
- Devices should have adequate and up-to-date anti-virus/malware software installed.

**Applies to Staff and Partners only (not Students):**

- In line with the College Data Breach procedure, it is important that individuals inform the Digital Services Helpdesk immediately if a mobile device (whether College owned or personal) that has been used to access College data is lost or stolen. The Digital Services Helpdesk will take steps to attempt to remotely wipe College data and apply measures to minimise the potential for data loss. The Digital Services Helpdesk will notify the Vice Principal People and Transformation, the Data Protection Officer, or a member of the Senior Leadership Team if a personal device containing data has been lost or stolen.
- It is strongly recommended that mobile devices are encrypted and are protected with a pin of at least 8 digits.
- Accessing College systems/data is not permitted on personal devices outside of the European Economic Area.
- Any application used on a mobile device must be downloaded from either the Apple App Store or Google Play Store (no 'jailbroken' devices should be used).
- Any devices accessing core or critical data/applications (HR data, Student Records, payroll) must be connected using a College encrypted laptop and Virtual Private network (VPN).
- If using a College owned mobile phone/tablet, the device must be enrolled in the Mobile Device Management system.
- Individuals should use College assigned storage to store, transfer, process, and access required data.
- PII data should never be sent outside of the College via email. If you need to send PII data external to the College then you must ensure:
  - There is a data sharing agreement in place.
  - The data file is suitably encrypted.
  - The data is shared and transferred using approved processes then unshared once the transfer has been completed.

## 6.4 Key Principles

### 6.4.1 Filtering

The College utilises automated recording, filtering, and monitoring software (Spam filter, URL filters, application filters, file auditing, administrative auditing software, etc.) to protect College systems, user data and other sensitive information. These cannot be guaranteed failsafe and users have a responsibility to be vigilant when using College systems and processing data.

Opening emails and browsing websites should always be carried out with diligence and care. The College will filter and attempt to scan and block content or Internet activity which is deemed as being unsuitable or malicious, containing viruses or exploits. This includes pornographic, gambling and sites that provide a security threat.

The College appreciates the cooperation from users and promotes a reporting culture with regards to Cyber incidents. Users are asked to inform Digital Services if they receive a suspicious email or notice irregular activity on their devices. Contact should be made to digitalservices@dumgal.ac.uk

### 6.4.2 Email

College email addresses and associated College email systems must be used for all official College business, to support audit purposes and institutional record keeping. All staff and students at the College must regularly read their College email and delete unwanted or unnecessary emails at regular intervals.

It is not permitted to use personal email accounts for work purposes at any time. Personal email accounts do not have the same level of security as College accounts and as such provide a serious risk to the Colleges networks.

### 6.4.3 Cyber Security

Cyber-attacks are an increasing threat to organisations. The attacks are mostly initiated through the theft of user credentials. Essentially attackers view people as being vulnerable and open to exploitation.

The College has taken steps to increase the understanding of staff around cyber security, which will ensure the College is better protected and that staff can better protect their personal digital identity outside of the College.

The College has introduced Multi Factor Authentication (MFA) for remote access on all College staff accounts. Use of MFA on personal accounts is strongly recommended (e.g., Gmail, Facebook, Twitter, and other social accounts).

Information relating to MFA will be routinely provided by the Digital Services Team.

### 6.4.4 Social Media

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.

Social Media 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 can be found in the social media guidelines in the quality manual on AdminNet and LearnNet.

### 6.4.5 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 e.g., 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 i.e., the intentional use of other people's material without attribution.

### 6.4.6 Monitoring

While the College Digital Services department aims to provide a high level of privacy all, users should be aware that the data they create on the College systems remains the property of the College.

Dumfries and Galloway College reserve the right to audit networks and systems on a periodic basis to ensure compliance with this policy. Systems are monitored to ensure that the confidentiality, integrity and availability of systems and data is maintained.

Users should be aware that data held within the College is not routinely inspected and user data will normally be treated as confidential. An examination of user data will only be carried out in response to an alleged violation to the AUP or for governance/legal reasons such as GDPR compliance or Police Investigation.

The College recognises that it has a duty of care in such investigatory work.
It should also be noted that when accessing College systems remotely your IP address is recorded and can be used responsibly by College security systems to prevent malicious activity; this can be with automated alerting systems or pro-actively by the Digital Services department.

The data the College collects, is subject to its processes and retention periods, these can be found in the College Data Protection Policy.
https://board.dumgal.ac.uk/dg_file/data-protection-policy/

Line managers of staff who leave the College will receive access to emails and files to ensure no important data is purged as a consequence of an individual leaving its employment.

To ensure business operations it may also be necessary to grant line managers access to staff files/emails if they are on prolonged sick or annual leave. Formal approval will be sought from SLT before access is granted.

### 6.5 Relevant Legislation

- Copyright, Designs and Patents Act 1988
- Malicious Communications Act 2003
- Computer Misuse Act 1990
- Trademarks Act 1994
- Data Protection Act 2018
- Human Rights Act 1998
- Regulation of Investigatory Powers Act 2000
- Freedom of Information (Scotland) Act 2002

### 6.6 External Guidance

National Cyber Security Centre, Cyber Essentials Plus Accreditation
https://www.ncsc.gov.uk/cyberessentials/overview

Scottish Government Public Sector Action Plan for Cyber Resilience
https://www.gov.scot/publications/cyber-resilience-strategy-scotland-public-sector-action-plan-2017-18/

## *7. Distribution*

All Staff
Repository

## 8. *Revision Log*

| Revision Log | | |
|---|---|---|
| Date | Section | Description |
| May 2023 | Throughout the Policy | Complete rework of policy to reflect current legislation and guidance |
| May 2023 | Throughout the Policy | Numbering changed to comply with Document Control Procedure |
| May 2023 | Distribution | Quality Manual changed to Repository |
| May 2023 | Responsibility | Job Title changed from Vice Principal Business Development and Corporate Services to Vice Principal, People and Transformation |
| June 2023 | Appendix | Student Friendly AUP Guidance Note added as Appendix 2 |

| **THIS FORM TO BE UPDATED WHENEVER THERE IS A CHANGE IN ANY SYSTEM DOCUMENT** | | | | |
|---|---|---|---|---|
| Document Name | Document Owner | Revision Number | Date of Issue | Date of Withdraw |
| ICT Acceptable Use Policy | Vice Principal, People and Transformation | 1 | | |

# Appendix 1: Equality Impact Assessment

| | |
|---|---|
| Document: | ICT Acceptable Use Policy |
| Executive Summary: | Impacts are positive across all of the protected characteristics for this policy as it will discourage online bullying and harassment or other inappropriate use which might create an intimidating culture within the college.<br><br>This applies less clearly to the additional considerations, although impacts should still be mildly positive as people from the groups listed can find themselves marginalised and excluded, which the policy should help to discourage.<br><br>The Human Right to privacy and family life is protected through restricted use of monitoring and data protection measures built into the policy. |

Duties:
1: Eliminate discrimination, harassment, and victimisation
2: Promote equality of opportunity
3: Promote good relations
* Human Rights to privacy and family life, freedom of thought and conscience, education, employment

PSED Impacts

| | Commentary |
|---|---|
| Age | The policy discourages online bullying and harassment, which can disproportionately affect people in minority groups across the protected characteristics. Prevention and reduced risk of this kind of negative behaviour will promote good relations. |
| Disability | |
| Gender | |
| Gender Based Violence | |
| Gender identity/ reassignment | |
| Marriage/civil partnership | |

| | |
|---|---|
| Pregnancy/maternity | |
| Religion or Belief | |
| Race | |
| Sexual Orientation | |

Additional Considerations

| | |
|---|---|
| Care experienced | The policy discourages online bullying and harassment, which can be a problem for people across the range of additional considerations as they can be marginalised and isolated.<br><br>The policy should encourage respect and instil confidence in people from these groups. |
| Carers | |
| Mental Health | |
| Socio-economic status | |
| Veterans | |
| Human Rights* | The Human Right to privacy and family life is protected through restricted use of monitoring and data protection measures built into the policy.<br><br>Rights to Education and Employment are positively impacted given that continued engagement in a course which might have been impacted by negative online behaviours of others is minimised. |

| | | | |
|---|---|---|---|
| Lead Officer: | Vice Principal, People and Transformation | | |
| Facilitator: | ICT Manager | | |
| Date initiated: | 06.06.23 | | |
| Consultation: | | | |
| Research: | | | |
| Signature | *Calum Rodgers* | Date | 28.08.23 |

## Appendix 2. Student Friendly AUP Guidance Note

This it to be displayed on the Student portal, linked in LearnNet and referenced in the student induction.

**The following acts will be considered misuse of College services and a breach of the ICT (Information and Communication Technology) Acceptable Use Policy:**

- **Installing any software without the permission of the ICT Department.**
- **Accessing in any form, unacceptable or offensive material including anything that can be considered racially, religiously, sexually, or politically offensive.**
- **Cyber- bullying or harassment in any form.**
- **Intentional damage to College ICT equipment.**
- **Intentionally affecting ICT security systems or the disruption of network.**
- **Using another user's login information to access College resources.**
- **Use of College systems for non-college related purposes.**
- **Use of College systems or equipment for any illegal activity.**

**All internet traffic is logged and monitored.**

**The full ICT Acceptable Use Policy can be found here: [LINK TO MAIN POLICY]**