Dumfries and Galloway College
One step ahead

ICT ACCEPTABLE USE POLICY

Responsibility: Director of Student Experience and Innovation

Issue Date: 23rd April 2026

Equality Impact Assessment: 14th April 2026

Version: 2

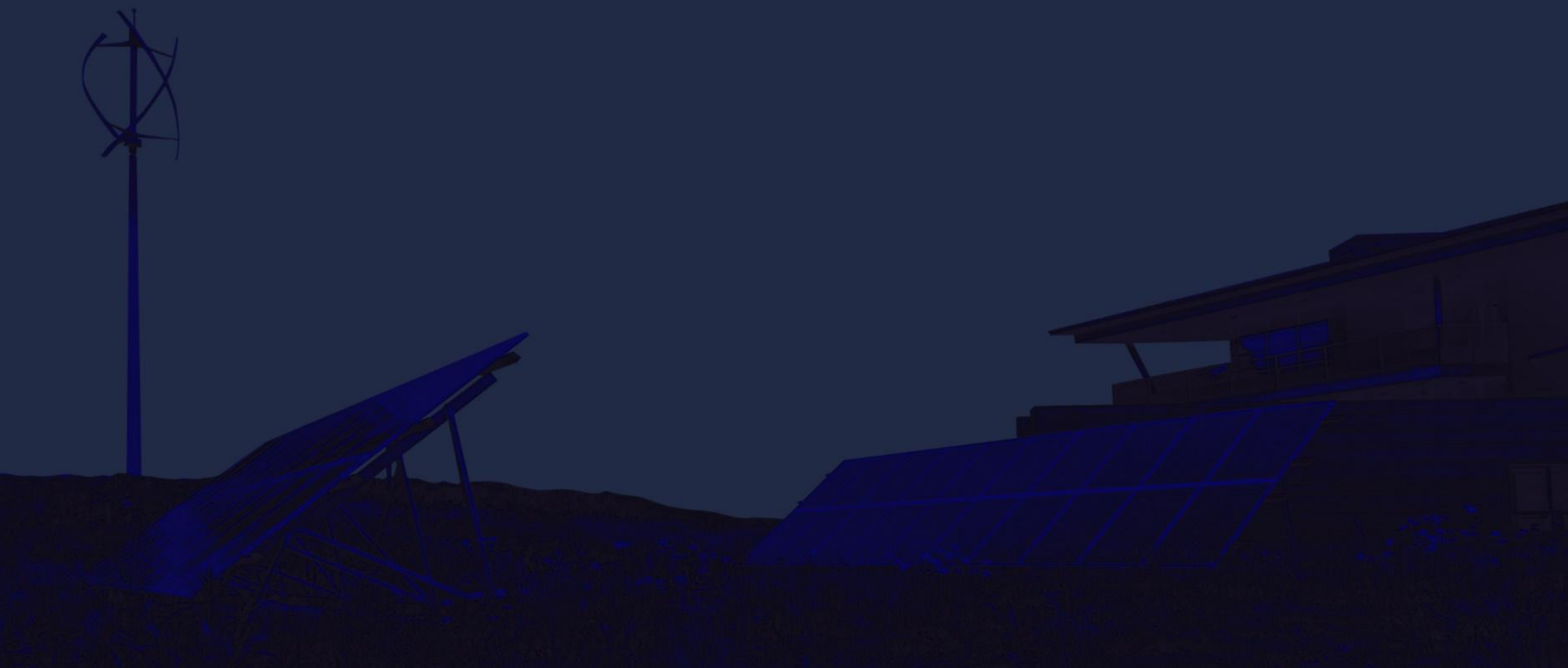

Table of Contents

ICT Acceptable Use Policy

1. Purpose

The purpose of this policy is to ensure that all users of Dumfries and Galloway College ICT systems use them in a safe, responsible and secure manner.

The College is committed to supporting staff and students in developing good digital practices. While misuse of systems may result in disciplinary action, the College recognises that many breaches arise from lack of awareness rather than malicious intent. As such, the College will take a proportionate approach, focusing on education, guidance and support wherever appropriate.

Deliberate, serious or repeated misuse will be addressed in line with College disciplinary procedures and, where necessary, may be referred to external agencies.

The aim of this policy is to support a culture of openness, trust and integrity, while protecting College systems, users and data from harm.

This policy defines the high-level principles and expectations for acceptable use. Detailed operational controls, technical standards and procedures are maintained separately and may be updated to reflect changes in technology, risk and regulatory requirements.

All internet access originating from the College network remains subject to the JANET Acceptable Use Policy.

2. Scope

The College recognises that staff and students have different roles, responsibilities and levels of access to ICT systems.

Controls and expectations will be applied proportionately, ensuring that security requirements do not create unnecessary barriers to learning while maintaining appropriate safeguards.

The College also recognises that some students may face barriers relating to access to devices, connectivity or digital skills. Where appropriate, reasonable adjustments will be made to support equitable access to College systems and services, in line with equality and inclusion principles.

3. References

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

- AI Policy
- Data Protection Policy
- Equality, Diversity and Inclusion Policy
- ICT Security Policy
- Data Protection Personal Data Breach Procedure
- Student Disciplinary Procedure

4. Definitions

Term	Definition
Acceptable Use Policy (AUP)	A set of rules defining how users are permitted to use College ICT systems, services and data.
ICT	Information and Communication Technology, including all systems, devices, networks and digital services used by the College
User	Any individual who accesses College ICT systems, including staff, students, contractors, partners and third parties
Account	A unique identity assigned to a user to access College systems and services.
Authentication	The process of verifying a user's identity before granting access to systems or data.
Multi-Factor Authentication(MFA)	An authentication method requiring two or more verification factors, such as a password and a mobile device or biometric.
Personal Data	Any information relating to an identified or identifiable individual, as defined under UK GDPR.
Sensitive Data	Information requiring a higher level of protection, including personal, confidential or restricted data.
Device	Any equipment used to access College systems, including desktops, laptops, tablets and mobile phones.
Bring Your Own Device (BYOD)	The use of personally owned devices to access College systems, services or data, subject to defined security controls.
Remote Access	Access to College systems and services from outside the College network.
Cloud Service	Any system or application hosted externally and accessed via the internet, including Microsoft 365 and other SaaS platforms.
Virtual Learning Environment (VLE)	The College's online learning platform (e.g. LearnNet) used to support teaching and learning.
Artificial Intelligence (AI)	Systems or tools that simulate human intelligence to perform tasks such as content generation, analysis or automation (e.g. ChatGPT, Copilot).

Spoofing	Impersonating another user, device or system to gain unauthorised access or deceive others.
Malware	Malicious software designed to disrupt, damage or gain unauthorised access to systems, including viruses, ransomware and spyware.
Phishing	A form of social engineering where fraudulent communications are used to trick users into revealing sensitive information.
Proxy/VPN	Technologies used to route network traffic through another system, sometimes used to bypass security controls.
Security Incident	Any event that compromises, or has the potential to compromise, the confidentiality, integrity or availability of systems or data.
Monitoring	The collection and review of system, network or user activity data for security, compliance or operational purposes.
Safeguarding	The protection of individuals from harm, abuse or exploitation, including within digital environments.
College Systems	All ICT systems, services, networks and applications owned, managed or provided by the College.
JANET	The UK's research and education network, governed by Jisc, providing internet connectivity to the College.

5. *Responsibility*

Role	Responsibility
Board of Management	Provide oversight of cyber security as a strategic risk. Significant cyber incidents, security posture updates, material risks, or compliance failures will be reported to the appropriate Board committee in line with the College's risk management framework.
Senior Leadership Team	Act as executive owner of the policy and ensure it remains aligned with strategy, legal requirements and risk management.
Digital Services Manager	Implement the policy through technical controls, procedures and standards, oversee security operations and compliance
Digital Services Staff	Maintain and operate secure systems, access is controlled and data handling, documentation and resilience measures are in place.
All Users	Follow the policy, protect College information, complete training and report incidents or suspicious activity

6. *Policy*

6.1 Disciplinary Procedures

The College will take a proportionate approach to breaches of this policy.

Where appropriate, issues will be addressed through guidance, support and education to promote safe and responsible use of ICT systems.

However, serious, deliberate or repeated breaches may result in:
- Removal or restriction of access to ICT systems
- Disciplinary action under relevant staff or student procedures
- Referral to external agencies where required

All actions will be taken in line with College policies and procedures and will

consider the intent, impact and risk associated with the incident.

6.2 Authorisation and Conditions of Use

6.2.1 Authorisation

Access to College ICT systems is provided to authorised users, including staff, students and approved third parties.

Access is granted based on role and is subject to appropriate controls.

By accessing College systems, users confirm their acceptance of this policy.

Access may be restricted, suspended or removed where misuse is identified or where required for security or operational reasons.

The College will ensure that access is provided in a fair and inclusive manner, making reasonable adjustments where required.

6.2.2 Conditions of Use

ICT resources and information systems are provided primarily to support teaching, learning, research and administrative operations.

Reasonable personal use is permitted, provided that such use does not interfere with College operations, compromise security, consume excessive resources, or breach College policies or applicable legislation.

All users are expected to act with integrity, responsibility and respect when using College ICT systems.

6.2.2.1 Data Risk Classification

Users must:

- Keep account credentials secure and not share them
- Use Multi-Factor Authentication (MFA) where required
- Report suspected account compromise immediately

Accounts are strictly personal and must not be shared.

Users are responsible for all activity carried out under their account.

Where users require support due to accessibility or additional needs, appropriate alternatives will be provided.

6.2.2.2 Acceptable Use and Behaviour

Users must:

- Communicate respectfully and professionally
- Use systems in a way that does not harm others or the College
- Comply with College policies, including equality and diversity standards

Users must not:

- Engage in harassment, bullying or discriminatory behaviour
- Access, store or share illegal, harmful or inappropriate material
- Use College systems for personal business, commercial gain or unlawful activity
- Install or use unauthorised software or services
- Attempt to bypass security controls

6.2.2.3 Network and System Integrity

Users must not:

- Attempt to bypass or weaken security controls
- Introduce malicious software or harmful content
- Disrupt or interfere with systems or network services
- Conduct unauthorised testing, scanning or monitoring activities

Only authorised devices and services may be connected to the College network.

6.2.2.4 Data Protection and Copyright

Users must comply with UK GDPR, the Data Protection Act 2018 and College policies.

Users must:

- Comply with UK GDPR, Data Protection Act 2018 and College policies
- Only access data necessary for their role
- Store and share data using approved systems only
- Protect personal and sensitive data at all times

Users must not:

- Transfer College data to personal storage or unapproved services
- Share personal or confidential data without authorization
- Copy or distribute copyrighted material without permission

Any suspected data breach must be reported immediately.

6.2.2.5 Use of Emerging Technologies

Emerging technologies, including artificial intelligence (AI), may be used where appropriate to support teaching, learning and operational activities.

Use of AI must:

- Be lawful, responsible and aligned with College policies
- Comply with awarding body requirements and academic integrity standards
- Not involve unauthorised processing of personal or confidential data

Misuse of AI in assessments may be treated as academic misconduct.

6.3 Accessing Services or Data Remotely

Users may access College systems remotely using approved services and devices.

The same standards of acceptable use apply whether accessing systems on campus or remotely.

6.3.1 General Requirements (All Users)

All users must:

- Ensure devices are maintained in a secure and up-to-date state
- Use secure authentication methods, including MFA where required
- Take appropriate precautions when using public or shared networks
- Access systems only through approved services and platforms
- Report loss, theft or compromise of devices or credentials immediately

6.3.2 Additional Requirements for Staff, Contractors and Partners

Staff and authorised partners must:

- Use secure and approved devices where required
- Ensure sensitive data is handled in line with College policies
- Use approved systems for storage and sharing of data
- Apply appropriate safeguards when working remotely

6.3.3 Students

Students may access College systems for learning and academic purposes.

Students must:

- Keep login credentials secure
- Use devices responsibly and securely
- Not attempt to bypass College security controls
- Report any issues or suspected compromise to Digital Services

The College recognises that some students may face barriers relating to access to devices or connectivity and will make reasonable adjustments where appropriate.

6.3.4 Security Monitoring and Compliance

The College applies monitoring in a proportionate, risk-based and transparent manner.

Monitoring is conducted to:

- Protect users and systems
- Support safeguarding
- Ensure legal and regulatory compliance

The College does not routinely monitor all user activity but reserves the right to investigate specific concerns where there is a legitimate reason to do so.

6.3.5 Summary

By accessing College systems remotely, users confirm that:

- Their access may be subject to monitoring in line with College policies
- They are responsible for maintaining the security of their devices and accounts
- They will comply with this policy at all times

6.4 Key Principles

The College provides access to ICT systems to support teaching, learning and operations.

All users share responsibility for protecting systems, data and users from harm.

6.4.1 Filtering and Threat Protection

The College uses layered security controls to protect systems and users from threats.

This may include filtering, malware protection and threat detection systems.

Users must remain vigilant and report any suspicious activity.

6.4.2 Email use and Communication Standards

College email must be used for official communication.

Users must:

- Use College email for official communication
- Communicate professionally and responsibly
- Take care when sending sensitive information

Users must not:

- Use personal email for College business
- Send malicious, misleading or inappropriate content

6.4.3 Cyber Security and Awareness

All users must:

- Remain aware of cyber security risks
- Complete required training where applicable
- Report suspicious emails or activity

The College promotes a culture of awareness and early reporting to protect the wider community.

6.4.4 Social Media and Online Conduct

Users must act responsibly when using social media.

Users must not:

- Damage the reputation of the College
- Share confidential or personal information
- Engage in harassment or offensive behaviour

6.4.5 Copyright and Intellectual Property and Compliance

Users must comply with copyright and intellectual property laws.

Users must not copy, distribute or use materials without appropriate permissions.

6.4.6 Monitoring and Privacy

The College respects user privacy and processes data in accordance with UK GDPR.

Monitoring is carried out in a proportionate and transparent manner to support security, safeguarding and compliance.

The College does not routinely monitor all user activity but may investigate specific concerns where required.

6.5 Relevant Legislation

This policy aligns with relevant legislation including:

- Data Protection Act 2018
- UK General Data Protection Regulation (UK GDPR)
- Computer Misuse Act 1990
- Copyright, Designs and Patents Act 1988
- Equality Act 2010

6.6 External Guidance

This policy is informed by national guidance including:

- National Cyber Security Centre (NCSC)
- Cyber Essentials and Cyber Essentials Plus
- Jisc JANET Acceptable Use Policy
- Information Commissioner's Office (ICO)
- Scottish Government Cyber Resilience Framework

7 Distribution

All Staff
All Students
Repository

8. Revision Log

Revision Log		
Date	Section	Description

24.03.2026	Throughout	Changes made throuhgout document to update in line with new Cyber Essentials, NCSC and Scot Gov requirements and recommendations
13.04.2026	Throughout	Change of language from Disciplinary to guidance and supporting.
14.04.2026	Equality Impact Assessment	Reworked to cover each individual point

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	Head of Corporate Services	1	12.11.20	
ICT Acceptable Use Policy	Director of Student Experience and Innovation	2	12.06.26	

Appendix 1: Equality Impact Assessment

Document:	ICT Acceptable Use Policy
Executive Summary:	This policy establishes the expectations for safe, responsible and respectful use of Dumfries and Galloway College ICT systems by all users. It supports a secure and inclusive digital environment by: • Promoting positive and respectful behaviour online • Protecting users from harm, including cyberbullying, harassment and misuse • Ensuring fair and proportionate application of rules and controls • Supporting equitable access to systems and services The policy recognises that users have differing levels of digital access, skills and confidence. As such, it promotes a supportive and educational approach, ensuring that controls and expectations do not unintentionally disadvantage any group. Security, monitoring and behavioural expectations are applied in a proportionate, transparent and inclusive manner, balancing safeguarding, security and individual rights.

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	Different age groups may have varying levels of digital literacy and awareness of acceptable use expectations. Risk:

	• Younger or less experienced users may unintentionally breach policy • Overly strict enforcement may disproportionately impact certain groups Mitigation: • Clear, accessible guidance provided • Educational and supportive approach prioritised over punitive measures • Proportionate enforcement based on intent and understanding
Disability	Users with disabilities may face challenges in accessing systems or complying with certain controls (e.g. MFA, device requirements, behavioural expectations in digital environments). Mitigation: • Reasonable adjustments provided where required • Compatibility with assistive technologies • Alternative methods of access or authentication available • Support from Digital Services
Gender	No direct negative impacts identified. Risk: • Misuse of ICT systems (e.g. harassment, inappropriate communication) Mitigation: • Clear behavioural expectations defined • Monitoring and reporting mechanisms support early intervention • Alignment with safeguarding and conduct policies
Gender Based Violence	Digital platforms may be used for harassment, coercion or abuse. Mitigation:

	• Policy explicitly prohibits abusive behaviour • Monitoring and safeguarding controls in place • Clear reporting and escalation pathways
Gender identity/ reassignment	No direct negative impact identified. Risk: • Potential misuse of communication platforms Mitigation: • Inclusive language and behaviour expectations enforced • Monitoring supports identification of inappropriate activity
Marriage/civil partnership	No impact anticipated
Pregnancy/maternity	No direct impact anticipated. Consideration: • Flexibility in access to systems and services Mitigation: • Remote access supported • No restrictive conditions that disadvantage access
Religion or Belief	Risk: • Filtering or content controls may unintentionally restrict access to legitimate material Mitigation: • Filtering applied proportionately • Review and exception processes available
Race	Risk: • Misuse of systems for discriminatory behaviour • Potential bias in monitoring or reporting processes Mitigation:

	• Policy explicitly prohibits discriminatory conduct • Monitoring and reporting processes support safeguarding • Staff training and oversight in handling incidents
Sexual Orientation	No direct negative impact identified. Mitigation: • Policy promotes respectful and inclusive behaviour • Safeguards in place to address harassment or discrimination

Additional Considerations

Care experienced	Users may have limited access to personal devices, stable environments or digital skills. Mitigation: • College-provided systems and facilities • Support and guidance available • Proportionate application of rules
Carers	Users with caring responsibilities may require flexible access. Mitigation: • Remote access supported • No unnecessary restrictions on when or how systems are accessed
Mental Health	Monitoring, enforcement or fear of disciplinary action may cause anxiety. Mitigation: • Transparent communication about monitoring • Emphasis on support and education • Proportionate response to breaches
Socio-economic status	Risk: • Digital poverty (devices, connectivity, access to resources) Mitigation: • Access to College systems and facilities

	• Reasonable adjustments for access issues • Avoidance of policies that assume high-end personal devices
Veterans	No direct impact identified. Mitigation: • Flexible access and support available where required
Human Rights*	This policy supports the Human Rights Act 1998 by: • Protecting the right to privacy through proportionate and transparent monitoring • Supporting freedom of expression within acceptable behavioural boundaries • Ensuring access to education and services through inclusive ICT provision • Balancing security, safeguarding and individual freedoms

Lead Officer:	Director of Student Experience and Innovation		
Facilitator:	Digital Services Manager		
Date initiated:	14th April 2026		
Consultation:	• Digital Services • Safeguarding / Student Services • Information Governance Group • Jisc / JANET guidance		
Research:	• Equality Act 2010 • UK GDPR and Data Protection Act 2018 • JANET Acceptable Use Policy • NCSC Cyber Security Guidance • Cyber Essentials / Cyber Essentials Plus • Jisc digital inclusion guidance		
Signature		Date	14.04.2026