Dumfries and Galloway College
One step ahead

ICT SECURITY POLICY

Responsibility: Director of Student Experience and Innovation

Issue Date: 23rd April 2026

Equality Impact Assessment: 24th March 2026

Version: 2

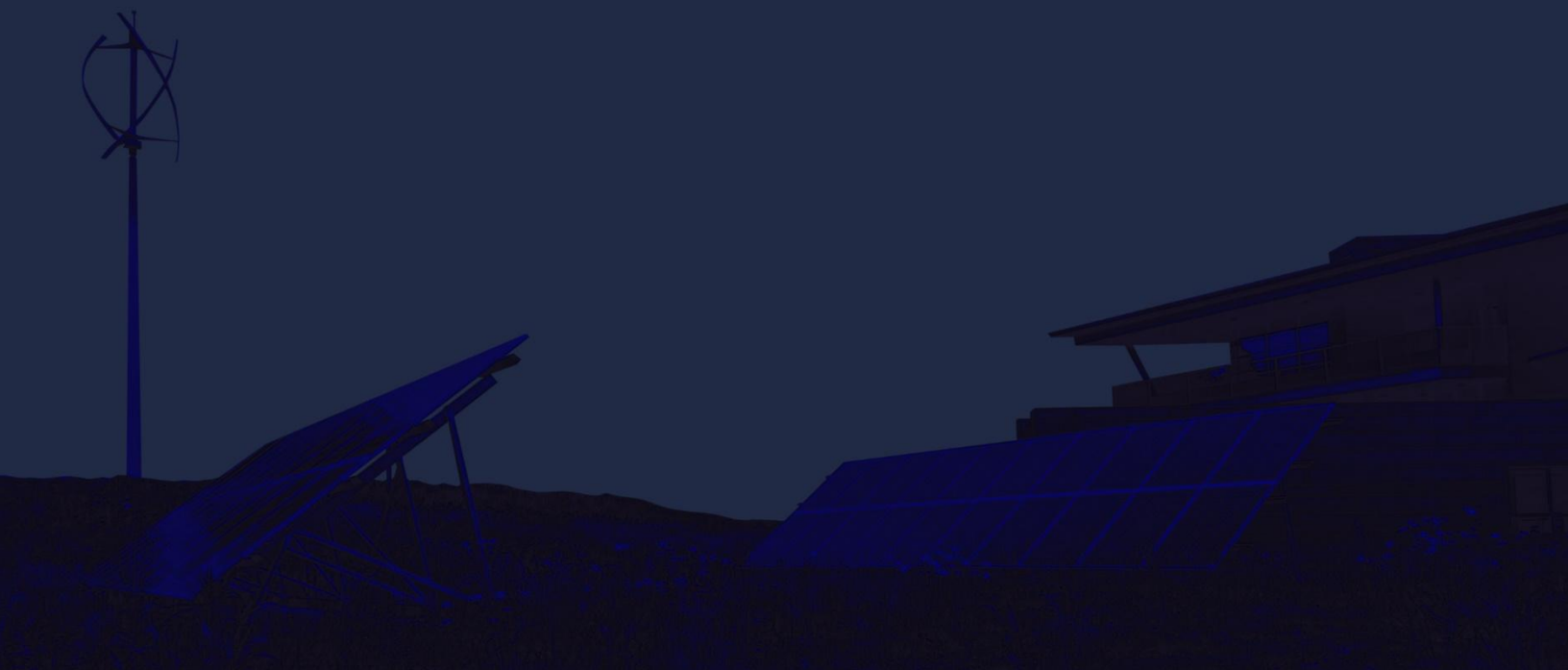

Table of Contents

ICT Security Policy

1. Purpose

The purpose of this policy is to define how Dumfries and Galloway College protects its information, systems and digital services against cyber threats.

The College operates in an increasingly complex digital environment, with growing reliance on cloud services, remote access, and interconnected systems. This policy establishes a clear framework to ensure the confidentiality, integrity and availability of College information, while supporting teaching, learning and business operations.

This policy aligns with recognised security standards and frameworks, including Cyber Essentials Plus and National Cyber Security Centre (NCSC) guidance. It sets

out the College's commitment to managing cyber risk, protecting personal data, and maintaining secure and resilient digital services.

All staff, students and third parties share responsibility for information security and must comply with this policy.

This policy defines the high-level principles and requirements for information security. Supporting standards, procedures and technical controls are maintained separately and provide detailed guidance on how these requirements are implemented in practice.

2. Scope

This policy applies across all Dumfries and Galloway College sites, systems and services, including on-premise infrastructure, cloud platforms, mobile services, remote access arrangements and third-party hosted services.

It applies to all staff, students, contractors, temporary staff, consultants, partner organisations and third parties who access, manage, support or process College information or use College digital services.

The policy covers College-owned devices, College-managed accounts, personal devices authorised to access College services, network infrastructure, servers, software, cloud platforms, data, backup systems and security monitoring services.

This policy applies regardless of where systems or data are accessed from, including College campuses, home working locations, mobile working arrangements and external partner sites.

Where third parties provide systems or services on behalf of the College, they must meet the relevant security, contractual, legal and regulatory requirements defined by the College. NCSC guidance also notes that BYOD introduces additional design, management and monitoring complexity, and that organisations should define clear responsibilities and controls before allowing it.

Controls and expectations will be applied proportionately, recognising differences between staff, students and third parties in terms of role, access, training and risk exposure.

3. References

This policy aligns with the following legislation, standards, frameworks and guidance:

3.1 Legislation and Regulatory Requirements

- UK General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018
- Privacy and Electronic Communications Regulations (PECR)
- Computer Misuse Act 1990
- Human Rights Act 1998

3.2 National and Government Guidance

- National Cyber Security Centre (NCSC) Cyber Security Guidance
- NCSC Cyber Essentials and Cyber Essentials Plus
- NCSC Zero Trust Architecture Principles
- NCSC Device Security and Bring Your Own Device (BYOD) Guidance

3.3 Standards and Frameworks

- NIST Cybersecurity Framework (CSF)
- NIST SP 800-53 – Security and Privacy Controls
- NIST SP 800-207 – Zero Trust Architecture

3.4 College Policies and Internal Documents

- Data Protection Policy
- ICT Acceptable Use Policy

- Risk Management Policy
- Business Continuity Management Plan

3.5 Sector-Specific Requirements

This policy supports sector-specific requirements and obligations associated with organisations including:

- Jisc (Janet Network),
- Scottish Awards Agency for Scotland (SAAS),
- Skills Development Scotland (SDS),
- Universities and Colleges Admissions Service (UCAS)
- Awarding bodies

The College ensures that information security controls support the secure exchange of data, compliance with funding and regulatory requirements, and the protection of learner and institutional data across these partnerships.

4. Definitions

Term	Definition
Access Control	The process of ensuring that only authorised individuals, systems or services can access specific resources, based on identity, role and security conditions.
Asset	Any data, device, system, application or service that has value to the College and requires protection.
Authentication	The process of verifying the identity of a user, device or service before granting access to systems or data.
Authorisation	The process of granting a user, device or service permission to access specific resources after authentication.
Bring Your Own Device (BYOD)	The use of personally owned devices to access College systems, services or data, subject to security controls and approval.

Cloud Service	Any system, platform or infrastructure hosted externally and accessed over the internet, including SaaS, PaaS and IaaS.
Cyber Incident	An event that compromises, or has the potential to compromise, the confidentiality, integrity or availability of information or systems.
Data Classification	The process of categorising information based on its sensitivity and the level of protection required.
Encryption	The process of converting information into a secure format that can only be accessed by authorised parties.
Endpoint	Any device that connects to College systems or services, including desktops, laptops, mobile devices and servers.
Identity and Access Management (IAM)	The framework of policies, processes and technologies used to manage digital identities and control access to systems and data.
Least Privilege	A security principle where users and systems are granted the minimum level of access required to perform their role.
Multi-Factor Authentication (MFA)	An authentication method requiring two or more verification factors, such as a password and a mobile device or biometric factor.
Personal Data	Any information relating to an identified or identifiable individual, as defined under UK GDPR.
Privileged Account	An account with elevated access rights, typically used for administrative or system-level functions
Remote Access	Access to College systems and services from outside the College network
Security Incident	Any suspected or confirmed event that may result in unauthorised access, data loss, system compromise or disruption to services
Service Owner	The individual responsible for ensuring that a system or service is managed securely and in line with College policies.

SIEM (Security Information and Event Management)	A system used to collect, analyse and monitor security events across the network to detect threats and support incident response.
Zero Trust	A security approach that assumes no implicit trust and requires verification of identity, device and contect for every access request

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 Core

- All persons involved with College ICT systems and information must read and comply with these policies.

6.2 Information Security

- The College will maintain a formal information security framework aligned to legal, regulatory and best practice requirements
- Information must be protected to ensure confidentiality, integrity and availability
- All information must be managed in line with legal, regulatory and contractual obligations

- The College will maintain and communicate security policies, procedures and standards
- All users must complete regular security awareness training

6.3 Data Risk Classification

The College operates a formal data classification scheme to ensure information is protected appropriately based on its sensitivity.
Information must be classified into one of the following categories:

- Highly Confidential – Sensitive personal data, safeguarding information, financial data, security credentials or information that could cause significant harm if disclosed.
- Confidential – Personal data, internal reports, commercially sensitive information.
- Internal – Routine operational information intended for internal use only.
- Public – Information approved for public release.
-

The information owner is responsible for assigning the classification.

Appropriate handling, storage, transmission and access controls must be applied based on classification level.

Guidance on handling requirements for each classification level will be provided in supporting procedures.

6.4 Data Handling

- Approved services must be used for storing, sharing and processing information
- Information must be securely created, stored, transmitted and deleted
- Services must define what classification of data they support
- Users must comply with defined procedures when handling data

6.5 User

If you use College managed, network connected devices and services, you must comply with the following:

6.5.1 Acceptable Use Policy

- Users must not share accounts or credentials
- Users must comply with data protection, licensing and legal requirements
- College email must be used for official business only
- Personal email must not be used for College business
- College devices must be used responsibly and lawfully
- Illegal, offensive or commercial misuse is prohibited
- Personal devices (BYOD) must be authorised and meet security requirements
- Users must report incidents, protect devices and maintain security
- The College may monitor usage for security and compliance purposes

6.5.2 User Password

- Passwords must be kept confidential and not shared
- Passwords must not be reused across systems
- Suspected compromised passwords must be reported and changed immediately
- Strong authentication, including MFA, must be used where required

6.5.3 Remote Working

- Remote access must be authorised and use approved methods
- College-issued or approved secure devices must be used wherever possible
- Devices must be encrypted and appropriately secured
- Secure authentication must be used for access
- Users must follow security guidance when working remotely

6.5.4 Clean Desk

- Sensitive information must be secured when not in use
- Devices must be locked when unattended
- Confidential materials must be stored securely
- Physical keys and access devices must not be left unattended

6.6 Management

6.6.1 Endpoint Security

6.6.1.1 Physical Security

- Access to critical infrastructure must be restricted to authorised personnel
- Visitors must be supervised at all times
- Environmental and power protections must be in place where required

6.6.1.2 Network Connection

- Only authorised devices may connect to the network
- Devices must meet defined security standards
- Network segmentation must be implemented where appropriate

6.6.1.3 End User Computing

- Devices must be centrally managed (e.g. Microsoft Intune)
- Devices must include firewall, endpoint protection (EDR), encryption and patching
- Devices must meet compliance standards before accessing College services

6.6.1.4 Server Management

- Servers must be securely configured and hardened
- Unnecessary services, accounts and protocols must be removed or disabled
- Administrative access must be restricted to authorised users
- Servers must include firewall, EDR, patching and encryption controls

6.6.1.5 Mobile Devices

- Mobile devices must use PIN, password or biometric protection
- Devices must be encrypted
- Devices must support remote wipe capability
- Devices should be centrally managed where possible

6.6.1.6 Bring Your Own Device (BYOD)

The use of personally owned devices (Bring Your Own Device – BYOD) to access College systems, services or data is permitted only where authorised and subject to defined security controls.

The College recognises that BYOD introduces additional risk and will apply proportionate controls based on the type of access, data classification and user role.

The following principles apply:

Authorisation and Access

- BYOD access must be explicitly authorised by the College
- Access will be restricted to approved services and systems
- Access may be limited based on user role, device type or security posture

Minimum Security Requirements
All personal devices used to access College systems must:

- Be protected by a PIN, password or biometric authentication
- Be configured with device encryption where supported
- Run a supported and up-to-date operating system
- Apply security updates in line with vendor guidance
- Not be jailbroken, rooted or otherwise compromised

Identity and Access Control

- Access to College services must use secure authentication methods, including Multi-Factor Authentication (MFA)
- Conditional Access policies may be applied to restrict access based on device compliance, location or risk level
- The College reserves the right to block or restrict access from devices that do not meet security requirements

Data Protection and Storage

- Highly Confidential or Confidential data must not be stored locally on personal devices unless explicitly authorised

- Approved College systems (e.g. cloud platforms) must be used for accessing and storing information
- Data must not be transferred to personal applications, storage or accounts

Monitoring and Enforcement

- The College may apply technical controls to enforce security requirements
- Access from BYOD devices may be monitored for security and compliance purposes
- Non-compliant devices may have access restricted or removed without notice

User Responsibilities

Users accessing College systems via personal devices must:

- Ensure their device meets the required security standards
- Protect their device from unauthorised access
- Report lost, stolen or compromised devices immediately
- Comply with all relevant College policies, including Acceptable Use and Data Protection

The College reserves the right to withdraw BYOD access where risks cannot be adequately managed.

BYOD access is primarily intended for low to moderate risk services such as email, collaboration tools and learning platforms.

6.6.2 Secure Configuration

6.6.2.1 Firewall

- Firewalls must operate a default deny policy for inbound traffic
- Management access must be restricted to authorised personnel
- All firewall changes must be documented, approved and risk assessed
- Firewall rules must be reviewed regularly

6.6.2.2 Malware Protection

- Endpoint protection solutions (e.g. Microsoft Defender) must be deployed
- Protection must be kept up to date
- Access to malicious websites must be blocked
- Additional controls such as sandboxing or application control may be implemented

6.6.2.3 Patch Management

- Systems must be patched regularly
- Critical security updates must be applied within defined timescales (e.g. 14 days)
- Only supported and licensed software may be used
- Non-compliant systems may be removed from the network

6.6.2.4 Identity and Access Management

- A central identity platform (e.g. Microsoft Entra ID) must be used
- Access must follow least privilege principles
- Multi-factor authentication must be enforced
- Administrative accounts must be separate and controlled
- Access must be reviewed regularly

6.6.2.5 Password Service Management

- Unique credentials must be used for all systems
- Passwords must not be transmitted in clear text
- Secure authentication methods must be used

6.6.2.6 Encryption

- Data must be encrypted at rest and in transit
- Approved encryption standards must be used
- Encryption keys must be securely managed
- Any exceptions must be risk assessed and approved

6.6.3 Service Lifestyle

6.6.3.1 Asset Management

- All assets must be recorded in an up-to-date register
- Asset records must be reviewed regularly

- Asset data must be protected from unauthorised change

6.6.3.2 Configuration Management

- Changes must be approved, tested and documented
- Risk assessments must be completed for changes
- Back-out plans must be defined
- Changes must be reviewed after implementation

6.6.3.3 Service Delivery Lifecycle

- Systems must follow secure development practices
- Development, test and production environments must be separated
- Security testing must be performed before deployment
- Post-implementation reviews must be conducted

6.6.3.4 Compliance

- The College must comply with all relevant legal and regulatory requirements
- Compliance must be documented and regularly reviewed

6.6.3.5 Disposal

- Data must be securely erased before disposal
- Disposal must be performed by approved providers
- Certificates of destruction must be retained

6.6.4 Detection

6.6.4.1 Monitoring

- Systems and networks must be monitored for suspicious activity
- Vulnerability scanning must be performed regularly
- Monitoring must be authorised and controlled

6.6.4.2 Logging

- Security logs must be collected centrally (e.g. SIEM/Wazuh)
- Logs must be protected from tampering
- Logs must be reviewed regularly

6.6.5 Response and Recovery

6.6.5.1 Incident Response

- Security incidents must be reported promptly
- Incidents must be managed through a defined process
- Post-incident reviews must be conducted

Incident response will involve all relevant stakeholders where appropriate, including the Data Protection Officer, Designated Safeguarding Lead, Senior Leadership Team and external partners.

Incidents involving personal data will be assessed in line with UK GDPR breach reporting requirements.

6.6.5.2 Business Continuity

- Business continuity plans must be documented
- Plans must be tested and reviewed regularly

Recovery priorities will consider the impact on teaching, learning, assessment delivery and learner support services, ensuring minimal disruption to the student experience.

6.6.5.3 Disaster Recovery

- Disaster recovery plans must meet defined recovery objectives
- Alternative recovery arrangements must be available

6.6.5.4 Backups

- Backups must be performed regularly
- Backups must be encrypted and protected
- Backup restoration must be tested
- Immutable backups should be used where possible

6.6.6 External Partnerships

6.6.6.1 Third Party

- Third parties must meet defined security requirements
- Risk assessments must be completed before engagement

- Access must be controlled and removed when no longer required
- Data must be protected in line with contractual obligations

6.6.6.2 Cloud

- Cloud services must be approved and centrally registered
- Full lifecycle risk assessments must be completed
- Data classification must determine suitability for cloud use

6.6.7 Supporting Procedures and Guidance

To support the implementation of this policy, the College maintains a suite of supporting procedures, standards and user guidance. These include, but are not limited to:

- User onboarding and induction guidance
- ICT Acceptable Use Policy
- Incident reporting procedures
- Data handling and classification guidance
- Bring Your Own Device Policy
- Access control and Identity management procedures

These documents provide practical, role-based instructions to ensure that all users understand their responsibilities and can comply with this policy effectively.

7. Distribution

-

All Staff
All Students
Repository

8. Revision Log

Revision Log		
Date	Section	Description
26.03.2026	Throughout	Updated in line with new legislation and guidelines
14.03.2026	Equality Impact Assessment	Updated to reflect individual impacts

24.04.2026	1. Purpose	Expanded to include UK GDPR, Data Protection Act 2018, PECR, Computer Misuse Act and Human Rights Act. Added NCSC Cyber Security guidance and Cyber Essentials Plus. Included NIST frameworks and Zero Trust principles. Added sector-specific obligations such as Jisc, SAAS, SDS, UCAS and awarding bodies. Shifted from internal references to full external regulatory alignment.
	2. Scope	Refocused from general ICT security to explicit cyber security and threat protection. Added alignment to Cyber Essentials Plus and NCSC guidance. Introduced a risk-based approach to protecting systems and data. Clarified separation between policy and supporting procedures. Expanded to include support for teaching, learning and business operations.
	3. References	Expanded to include cloud services, remote working, mobile and personal devices, and third-party hosted systems. Clarified applicability across all locations including on-site and remote access. Expanded coverage to include staff, students, contractors and partners. Introduced a proportionate control approach based on user type and risk.
	4. Definitions	Expanded to include modern cyber security terminology including MFA, Zero Trust and SIEM. Added definitions for cloud services, BYOD and identity and access management. Clarified distinction between cyber incidents and security incidents. Improved clarity and consistency of terminology.
	5. Responsibility	Updated governance structure to include Board of Management oversight. Expanded Senior Leadership Team accountability. Replaced ICT Manager role with Digital Services Manager. Clarified responsibilities for Digital Services staff and all users. Strengthened accountability and reporting lines.
	6. Procedure	Introduced requirement for a formal information security framework. Added requirement for regular security awareness training. Formalised data classification model. Strengthened compliance requirements.
	6.2 User	Strengthened acceptable use expectations and restrictions on personal email use. Introducing mandatory multi-factor authentication where required. Enhanced password and authentication controls. Strengthened remote working requirements including use of secure devices. Improved clarity on user responsibilities and incident reporting.
	6.3 Management	Expanded controls to include central device management and endpoint protection requirements. Strengthened server hardening and access restrictions. Added network segmentation requirements. Introduced formal BYOD

		controls. Strengthened patching timelines, encryption requirements and identity and access controls.
	6.4 Supporting Procedures and Guidance	New section introduced. Formalised supporting procedures, operational standards and user guidance. Clarified that detailed implementation sits outside the policy.
	7. Distribution	Expanded distribution from staff only to include staff and students.
	8. Revision Log	Updated to reflect full policy refresh aligned to legislation and guidance. Included updated Equality Impact Assessment.
	Appendix: Equality Impact Assessment	New appendix introduced. Covers accessibility, inclusion and usability impacts. Includes risks such as MFA barriers and digital access issues. Provides mitigation measures and promotes a balanced approach between security and usability.

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 Security Policy	Head of Corporate Services	1	12.11.20	
ICT Security Policy	Director of Student Experience and Innovation	2	23.04.26	

Appendix 1: Equality Impact Assessment

Document:	ICT Security Policy
Executive Summary:	This policy outlines Dumfries and Galloway College's approach to protecting its ICT systems, users and data through secure, proportionate and risk-based controls. The policy supports a safe and inclusive digital environment by ensuring that security measures protect individuals from harm, including cyber threats, data breaches, and misuse of systems, while maintaining equitable access to digital services. Key objectives include: • Protecting users and systems from cyber threats • Ensuring lawful, fair and transparent use of monitoring and security controls • Supporting users with differing levels of digital access, skills and confidence • Applying security controls proportionately to avoid unnecessary barriers The College recognises that security measures must be balanced with usability, accessibility and inclusion. As such, the policy promotes education, support and reasonable adjustments to ensure all users can safely and effectively access ICT services.

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	Security controls such as MFA, password requirements and device compliance may present usability challenges for some users. Mitigation: • Provide clear guidance and support for all age groups • Ensure training materials are accessible and easy to follow • Apply controls proportionately based on risk
Disability	Security measures (e.g. MFA apps, device compliance, monitoring tools) may create accessibility barriers. Mitigation: • Ensure compatibility with assistive technologies • Provide alternative authentication methods where required • Offer reasonable adjustments and support through Digital Services
Gender	No direct negative impacts identified. Risk: • Online harassment or misuse of systems Mitigation: • Policy explicitly prohibits harassment and inappropriate behaviour • Monitoring and reporting mechanisms support early intervention
Gender Based Violence	Digital platforms could be used for harassment or abuse. Mitigation: • Monitoring and safeguarding controls in place • Clear reporting and escalation processes

	• Alignment with safeguarding policies
Gender identity/ reassignment	No direct impact identified. Risk: • Misuse of systems leading to discrimination or harassment Mitigation: • Inclusive behaviour expectations enforced • Monitoring supports identification of inappropriate activity
Marriage/civil partnership	No impact anticipated
Pregnancy/maternity	No direct impact anticipated. Consideration: • Flexibility in remote access and secure working arrangements Mitigation: • Secure remote access supports continued participation • No restrictive controls that disproportionately impact access
Religion or Belief	No direct negative impact identified. Risk: • Filtering or monitoring tools may inadvertently restrict access to legitimate content Mitigation: • Filtering applied proportionately • Exceptions and review processes available
Race	Risk: • Bias in monitoring or automated security tools (e.g. anomaly detection, AI-driven filtering) Mitigation:

	• Use of trusted, compliant security solutions • Oversight of monitoring practices • Staff training on bias and appropriate use of tools
Sexual Orientation	No direct negative impact identified

Additional Considerations

Care experienced	Users may have limited access to personal devices or stable environments. Mitigation: • College-provided devices and systems • Flexible access arrangements • Support through Digital Services
Carers	Users with caring responsibilities may require flexible access. Mitigation: • Secure remote access available • No unnecessary restrictions on time/location of access
Mental Health	Security controls (e.g. monitoring, restrictions, authentication requirements) may cause stress or anxiety. Mitigation: • Transparent communication about monitoring • Proportionate enforcement • Support-focused approach rather than punitive
Socio-economic status	Risk: • Digital poverty (devices, connectivity, capability) Mitigation: • College systems designed to work across a range of devices • On-site access available • Support and guidance provided
Veterans	No direct impact identified

Human Rights*	This policy supports the Human Rights Act 1998 by: • Protecting the **right to privacy** through secure handling of personal data • Ensuring monitoring is lawful, proportionate and transparent • Supporting **access to education and employment** through secure systems • Balancing security with individual freedoms

Lead Officer:	Director of Student Experience and Innovation		
Facilitator:	Digital Services Manager		
Date initiated:	24 March 2026		
Consultation:	• Digital Services • Information Governance Group • Safeguarding / Student Services • Jisc / NCSC guidance		
Research:	• UK GDPR and Data Protection Act 2018 • Equality Act 2010 • NCSC Cyber Security Guidance • Cyber Essentials / Cyber Essentials Plus • Jisc Security & Acceptable Use frameworks		
Signature		Date	24.03.2026