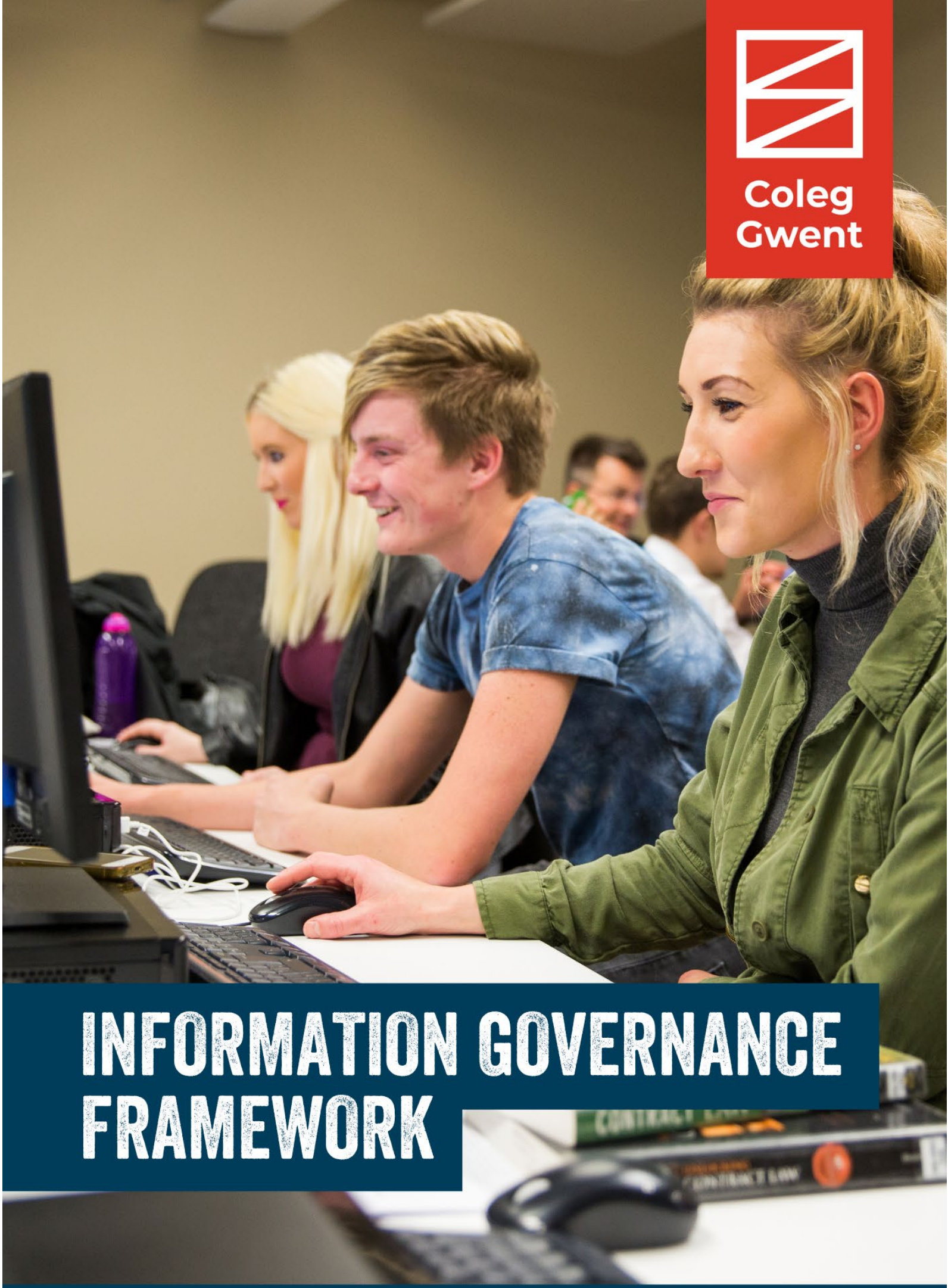


Coleg Gwent

INFORMATION GOVERNANCE FRAMEWORK

Information Governance Framework

Equality Impact Assessment:	March 16th 2026
Approved by:	The Corporation and in consultation with the Trade Unions
Tier:	1
Author:	Diane Clark, Director of ICT
Date Approved:	07/07/2026
Review Date:	07/2027
Published on:	Website Staff Intranet CG Connect
Accessibility:	Available in large font and other formats on request

Contents

INFORMATION GOVERNANCE FRAMEWORK

1 Introduction 1
2 Purpose and Scope 1
3 Framework Structure 2
4 Shared Responsibilities of the College and Its Users 2
5 Governance, Roles and Accountability 3
6 Education, Guidance and Support 5
7 Monitoring, Safeguarding and Privacy 6
8 Reporting Concerns and Incidents 8
9 Consequences of Non-Compliance 9
10 Legal and Regulatory Context 10
11 Review and Availability 10

ACCEPTABLE USE POLICY

1 Policy Statement 11
2 Purpose and Scope 11
3 Standards of Use and Behaviour 11

E-SAFETY POLICY

1 Policy Statement 13
2 Purpose and Scope 13
3 Standards of Use and Behaviour 13

INFORMATION SECURITY POLICY

1 Policy Statement 15
2 Purpose and Scope 15
3 Information Security Principles 15
4 Information Security Commitments 15

DATA PROTECTION POLICY

1 Policy Statement 18
2 Purpose and Scope 18
3 Data Protection Principles 18
4 Data Protection Commitments 19

INFORMATION GOVERNANCE FRAMEWORK

1 Introduction

This Framework explains how the College governs the secure, lawful and responsible use of information and digital technologies. It explains the overarching principles, accountabilities and risk-based approach that underpin information security, data protection, online safety and the use of College ICT in support of teaching, learning and day-to-day operations.

For the purposes of this Framework, the College refers to Coleg Gwent, including all campuses, services, and business functions. This Framework also applies, where relevant, to contractors and subcontractors acting on behalf of the College, in accordance with their contractual obligations.

For the purposes of this Framework, *College ICT* includes all systems, services, networks, equipment, devices, user accounts and information, whether College-owned, provided by third parties, or personally owned where authorised for College use.

Effective information governance enables the College to:

- protect learners, staff, governors and other users
- safeguard information, systems and user accounts
- reduce the risk of harm, data loss, misuse and criminal activity
- meet legal, regulatory and contractual obligations
- protect the College's reputation and integrity

2 Purpose and Scope

This framework explains the College's mandatory expectations for the secure and responsible use of College ICT. It defines roles and responsibilities, sets the College's overarching approach to information governance and risk management, and underpins compliance with relevant legislation, regulatory requirements and recognised standards.

This Framework is informed by the College's Risk Management Policy and associated risk appetite, which establishes a zero-tolerance position in relation to Information Governance risks. This reflects the College's safeguarding responsibilities and its legal and regulatory obligations, particularly in relation to data protection, information security and online safety.

Unless explicitly stated otherwise, all policies within this Framework apply to all users and to the use of College ICT, regardless of location or device ownership.

- **People**: all learners, staff, governors, contractors, subcontractors and others acting on behalf of the College
- **Technology**: all physical and virtual College ICT

- **Information**: all information the College creates, receives or manages, in any format

Where appropriate, it also applies to prospective learners, parents or carers and other individuals who interact with College ICT, in line with the nature and extent of that interaction.

The College applies a risk-based and proportionate approach to information governance, taking account of safeguarding duties, legal obligations, and the level of risk the College is prepared to accept. Information governance arrangements also support business continuity and disaster recovery planning.

This framework forms part of the College's wider governance framework and must be applied alongside relevant policies, procedures and codes of conduct. Compliance with this Framework and its supporting policies is a condition of employment, enrolment, or engagement with the College, as applicable and in accordance with College procedures and applicable law.

3 Framework Structure

The Framework brings together the College's Tier 1 policies covering the following areas:

- **Acceptable Use Policy** – how College ICT systems and information may be used
- **E-Safety Policy** – staying safe online and communicating respectfully
- **Information Security Policy** – protecting systems, accounts and information
- **Data Protection Policy** – lawful and secure handling of personal data

Each policy retains its distinct purpose and scope. This Framework provides the overarching governance, principles and shared expectations that apply across all policies, including arrangements for training, monitoring, reporting, compliance and risk management.

This approach avoids duplication and promotes consistency in how information governance risks are managed.

Where requirements overlap or conflict, safeguarding and legal obligations take precedence, followed by data protection and information security requirements.

4 Shared Responsibilities of the College and Its Users

This section explains the shared responsibilities of the College and its users in relation to the secure and responsible use of College ICT. It reflects the College's commitment to acting lawfully, proportionately and with appropriate support, while making clear what is expected of all users.

The College will:

- provide secure College ICT
- set clear expectations and provide appropriate training, education and guidance

- apply proportionate technical and organisational security controls
- identify, manage and review information security risks
- respond promptly and proportionately to incidents and concerns
- work with suppliers and partners who meet defined security and data protection requirements
- act lawfully and proportionately

All users are expected to:

- use College ICT safely, lawfully and responsibly
- protect login credentials and safeguard College information and personal data
- behave respectfully and professionally online
- report concerns, incidents or suspected breaches promptly
- seek advice or support when unsure

5 Governance, Roles and Accountability

This section explains how information security, safeguarding, and data protection risks are governed across the College, including how risk appetite is defined, accountability is assigned, and decisions are made where interpretation, exceptions, or risk acceptance are required.

5.1 Risk Appetite and Senior Oversight

The College's risk appetite for information governance and data protection is set by the Governing Body through the Corporate Risk Register, in accordance with the College's Risk Management Policy.

Senior oversight ensures that risks are identified, assessed and managed in line with the College's safeguarding responsibilities, legal obligations, and strategic priorities. Where risks exceed the agreed risk appetite, or where potential impact is significant, they are escalated to the Corporate Leadership Team (CLT) and, where appropriate, to the Governing Body through the Audit Committee.

5.2 Governance Roles and Responsibilities

Clear roles and responsibilities support effective governance of information security, safeguarding, and data protection. Key roles include:

- **Governing Body** – receives assurance that proportionate and effective arrangements are in place to manage related risks
- **Corporate Leadership Team (CLT)** – provides senior oversight and considers significant risks, incidents and assurance reports
- **Director of ICT** – owns this framework and has authority over its interpretation, the approval of exceptions, and the acceptance of information security risk. HR oversight applies where

staff conduct, monitoring, or employment outcomes may be affected, with CLT escalation for novel or high-risk matters

- **Managers** – embed framework requirements into day-to-day practice
- **Safeguarding Team** – manages safeguarding and Prevent-related concerns, including those arising from digital activity
- **Head of Infrastructure & Security** – operates technical controls and investigates information security incidents
- **Data Protection Officer (DPO)** – oversees data protection compliance and personal data breach management

5.3 User Accountability and Proportionality

Users are responsible for all activity carried out using their account unless there is evidence of compromise or unauthorised access.

The College recognises that users have differing levels of digital experience, confidence and support needs. When concerns arise, a clear distinction is made between:

- genuine error, misunderstanding or lack of awareness; and
- deliberate, reckless or repeated non-compliance.

For example, a one-off mistake arising from a lack of awareness would normally be addressed through guidance or training, whereas deliberate or repeated disregard for security requirements may require more formal action.

Issues are addressed fairly and proportionately, with education, guidance, and support used as the primary response wherever appropriate, particularly for learners.

5.4 Exceptions and Risk Acceptance

What an exception is

In rare and justified circumstances, the College may approve an exception to this Framework or its supporting policies where this is necessary to support legitimate College activity. An exception represents the formal acceptance of a clearly defined risk for a specific purpose and a limited time period.

An approved exception does not mean the College has accepted unmanaged risk; it means the risk has been assessed, mitigated where possible, formally approved and kept under review for a defined purpose and period.

By way of example, an exception may be approved to permit the time-limited use of a system or service that does not fully meet College cyber security standards. Such an exception would be considered only where it is necessary to support essential College activity and where appropriate risk assessment, mitigating controls and formal approval are in place.

Approval of exceptions

All exceptions must be:

- risk assessed and clearly understood
- formally approved in advance by the Director of ICT or an authorised delegate
- recorded to support consistency, transparency and auditability

Where a proposed exception represents a significant, unusual or higher-risk departure from this framework or exceeds the College's risk appetite, it will be escalated to the Corporate Leadership Team (CLT) for consideration

What an exception does not allow

Exceptions must be formally approved in advance. Informal, local, implied or retrospective approvals are not valid and must not be relied upon.

An approved exception:

- applies only to the specific activity, purpose and time period for which it has been approved
- does not remove the requirement for appropriate safeguards, mitigating controls or ongoing oversight
- does not change or override College policies more generally
- does not create a precedent or entitlement to future expectations
- must not be extended, reused or applied in any other systems, service, activity or context

Decision making

Decisions relating to interpretation, exceptions or risk acceptance are made using professional judgement, informed by evidence and consideration of potential impact on individuals and the College. Decisions follow College procedures and principles of fairness and proportionality.

6 Education, Guidance and Support

This section focuses on how the College supports users to understand and meet information security, safeguarding, and data protection requirements through proportionate education, guidance, and ongoing support.

6.1 Purpose of Education and Support

Education and guidance are central to the College's information governance and safeguarding approach. They support the safe, confident, and responsible use of technology and information, and help to:

- reduce the likelihood of incidents and harm
- promote consistent and responsible behaviour
- distinguish genuine error from deliberate or repeated non-compliance

Education and support are intended to prevent issues arising and to help users work safely and confidently, rather than to punish mistakes.

6.2 Proportionate and Role-Based Approach

Training and guidance are provided on a proportionate basis, taking account of:

- role, responsibilities and system access
- the nature and sensitivity of information handled
- safeguarding and online safety risks
- differing levels of experience, confidence and support needs

For example, users with elevated system access or responsibility for sensitive information may be required to complete additional or more frequent training.

Induction, refresher training and role-specific guidance are tailored so that expectations are clear, realistic and achievable in practice.

6.3 Framework Scope and Supporting Materials

This Framework is intentionally focused on Tier 1 principles, governance, roles and expectations. Detailed operational content, including procedures, technical standards and step-by-step guidance, is maintained separately and communicated through:

- induction and refresher training
- role-specific briefings and resources
- College guidance and intranet materials

This approach ensures the Framework remains stable and strategic, while enabling supporting materials to evolve in line with technology, risk and practice.

6.4 User Responsibilities

All users are expected to:

- engage with required learning and issued guidance, as appropriate to their role or access
- complete mandatory training as directed, where applicable to their role or access
- apply training and advice in day-to-day use of systems and information
- seek advice or support where requirements are unclear or uncertain
- raise concerns or questions promptly rather than acting outside guidance

The College encourages users to raise questions or seek support early, recognising that this helps prevent issues escalating and supports safer practice

7 Monitoring, Safeguarding and Privacy

The College may monitor the use of its ICT where necessary to protect learners, staff, systems and information, while respecting privacy, proportionality and legal requirements. Monitoring is a protective and preventative measure to reduce risk and harm, and is not intended as routine or punitive surveillance.

7.1 Purpose and Scope of Monitoring

The College monitors use of College ICT to:

- protect learners, staff and other users
- safeguard College ICT
- prevent, detect and where necessary investigate misuse, fraud or criminal activity
- meet legal, regulatory and safeguarding obligations

Monitoring applies to College ICT and does not involve continuous or routine surveillance of individual learners or staff.

7.2 Lawful Basis and Authorisation

Monitoring is carried out under appropriate lawful bases, including:

- the College's legitimate interests
- compliance with legal and regulatory obligations
- the protection of vital interests, where applicable

Where monitoring activity is likely to result in a heightened risk to individuals' rights or freedoms, a Data Protection Impact Assessment (DPIA) is completed in line with data protection requirements.

Access to monitoring information, and decisions to review individual activity, are restricted to authorised staff and subject to appropriate approval.

7.3 How Monitoring is Applied

The College's approach to monitoring:

- is proportionate and risk-based
- relies primarily on automated controls
- is targeted at specific, clearly identifiable security, safeguarding or legal risks, rather than general user behaviour

Automated security systems operate continuously to protect College ICT. Monitoring is not used for performance management, attendance monitoring, or routine supervision of learners or staff.

7.4 Review of Individual Activity

Review of individual activity is an exceptional measure and will only take place where there are specific and justified grounds for concern. These may include:

- safeguarding or online safety concerns
- suspected misuse of College ICT
- security incidents or system alerts
- a lawful request from an external authority

Any review of individual activity requires authorisation from the Corporate Leadership Team (CLT) and is conducted in compliance with UK GDPR, the Data Protection Act 2018, and related legislation.

CCTV operates separately for site safety and crime prevention and is governed by the College's CCTV Policy.

8 Reporting Concerns and Incidents

This section explains how concerns and incidents relating to information security, safeguarding, online safety, and data protection should be reported and managed to reduce risk and prevent harm.

8.1 What Must be Reported

All users must report suspected or actual concerns relating to:

- misuse of College ICT or account compromise
- cyber security incidents, including phishing or malware
- personal data breaches or near misses
- online safety or safeguarding concerns
- suspected or actual security, data protection or safeguarding breaches involving third parties

Where there is an immediate risk of harm to an individual, emergency services must be contacted without delay.

8.2 How to Report

The College provides multiple reporting routes to ensure concerns can be raised promptly and appropriately. Concerns must be reported through the most relevant College route, including:

- **ICT Help Desk or ICT Team** – misuse of College ICT and security concerns
- **Safeguarding Team** - safeguarding and online safety concerns
- **Data Protection Officer** - data protection and personal data breaches
- **Line management or other designated College reporting routes** - where appropriate

Reporting routes are communicated through College procedures, guidance and training.

8.3 How Reports are Handled

All reports are:

- handled sensitively and proportionately
- recorded in line with College procedures
- assessed by appropriate specialist teams

Information is shared only with those who need to know in order to manage the concern, meet legal and regulatory obligations, and reduce the risk of harm.

8.4 Protection for Those Raising Concerns

Individuals will not be disadvantaged for raising concerns in good faith. The College promotes a culture in which concerns can be raised safely and responsibly, and supports those who report issues relating to safeguarding, security or data protection.

Concerns relating to fraud, financial irregularity or serious wrongdoing may also be raised under the College's Anti-Fraud and Whistleblowing Policy.

9 Consequences of Non-Compliance

This section explains how the College responds fairly and proportionately where this Framework or its associated policies are not followed.

9.1 Principles for Addressing Non-Compliance

Where non-compliance occurs, the College responds in accordance with the following principles:

- protection of learners, staff and others from harm
- safeguarding and legal obligations
- proportionality and fairness
- learning, prevention and improvement wherever possible

9.2 Differentiating Error from Misconduct

When concerns arise, the College distinguishes between:

- **genuine mistakes or misunderstanding**, where education, guidance or additional support is the most appropriate response; and
- **deliberate, reckless or repeated non-compliance**, where more formal action may be required.

9.3 Actions the College May Take

Where non-compliance is identified, the College may take one or more of the following actions, depending on the circumstances:

- provision of additional guidance, training or support
- corrective or remedial action to reduce risk or prevent recurrence
- temporary or permanent restriction of access to College ICT
- management, capability or disciplinary action, in line with relevant College procedures
- referral to external authorities where required by law or safeguarding obligations

Any action taken will be justified and proportionate to the nature and seriousness of the issue.

9.4 Safeguards and Fair Treatment

All actions relating to non-compliance are undertaken:

- in accordance with College policies and procedures
- with appropriate oversight and authorisation
- with due regard for fairness, confidentiality and data protection
- recognising the College's duty of care to learners and staff

Where learners are involved, responses take account of safeguarding responsibilities and educational context, with support and wellbeing prioritised.

Where matters involving staff progress beyond informal guidance or support, any formal action will be managed solely through the College's established HR policies and disciplinary procedures.

10 Legal and Regulatory Context

These legal and regulatory requirements underpin the College's approach to safeguarding, data protection and information security and inform how this framework is applied in practice.

- UK GDPR and the Data Protection Act 2018
- Computer Misuse Act 1990
- Regulation of Investigatory Powers Act 2000 and Investigatory Powers Act 2016
- Counter-Terrorism and Security Act 2015 (Prevent duty)
- Online Safety Act 2023
- Data (Use and Access) Act 2025
- Equality Act 2010

This list is not exhaustive and reflects legislation in force at the time of approval.

11 Review and Availability

The framework and associated policies are reviewed annually, or sooner where required by changes in law, technology or risk.

The College uses incidents, audits and feedback to support continual improvement of its information governance arrangements.

ACCEPTABLE USE POLICY

1 Policy Statement

The College is committed to ensuring that College ICT is used in a safe, lawful and responsible manner. Appropriate use of technology supports teaching, learning and day-to-day operations and helps protect learners, staff, and the College's information assets and reputation.

2 Purpose and Scope

This policy:

- defines acceptable and unacceptable use of College ICT
- sets user responsibilities for keeping accounts, systems, and data safe
- supports legal and regulatory compliance and the College's wider policies

Reasonable adjustments or additional support may be provided to enable appropriate and responsible use of College ICT, in line with College policies and legal obligations.

This policy forms part of the Information Governance Framework and must be read and applied in conjunction with it.

3 Standards of Use and Behaviour

These requirements focus on the secure, lawful and authorised use of College ICT.

3.1 What You Must Do:

- use only your own College account and keep passwords confidential
- enable multi-factor authentication (MFA) where provided
- report any suspected compromise (for example, lost or stolen devices, phishing, or unusual activity) as soon as possible
- use College ICT only for lawful, authorised and appropriate purposes
- use your College email account for College business
- ensure any personal use of College ICT is reasonable, infrequent, and incidental, and does not interfere with work or learning, system performance, security, or College operations
- comply with external terms and conditions where applicable (for example, the JANET Acceptable Use Policy)
- install only ICT-approved software and connect only ICT-approved hardware
- keep College devices physically secure and lock screens when unattended
- enrol personal devices in College-approved device management where required; this may include the application of security settings and the remote removal of College data
- store College information only in approved College ICT storage locations, and not in

personally owned devices or cloud accounts

- apply encryption or password protection when sending personal or sensitive data
- comply with copyright and licensing requirements
- prevent casual or unauthorised disclosure of information
- retain information only for as long as required
- dispose of information securely in line with College procedures

3.2 What You Must Not Do

- ask for, use, or share anyone else's credentials, or share your own credentials
- log in for another user or ask another user to log in for you
- allow anyone else to use a device or system while you are signed in, including leaving a device signed in for another person to use
- access any account, system, or data without explicit authorisation
- attempt to bypass, disable or weaken security controls
- interfere with the operation of systems or networks
- carry out security testing or probing without authorisation
- access, create, store, or share content that is illegal, discriminatory, harassing, extremist, obscene, defamatory, or likely to bring the College into disrepute
- use unapproved services (including personal accounts) to store or share College information
- use public or unsecured networks to access College ICT unless approved secure access methods or controls are in place
- undertake activities that expose the College or its users to security, safeguarding, or reputational risk
- record, photograph or otherwise capture individuals without their knowledge and appropriate authorisation; covert recording is prohibited
- store College personal or sensitive data locally on personal devices

E-SAFETY POLICY

1 Policy Statement

The College is committed to the E-Safety and wellbeing of all learners, staff and members of the College community when using digital technologies and online platforms. E-Safety is a core part of safeguarding and underpins the College's responsibility to protect individuals from online harm.

2 Purpose and Scope

This policy exists to:

- promote the safe, responsible and ethical use of digital technologies across the College
- protect users from online risk and harm
- maintain clear professional boundaries between staff and learners
- support compliance with safeguarding, Prevent, data protection and related requirements
- safeguard the College's reputation and digital presence

The College recognises that online risks may affect users differently depending on age, experience and individual circumstances. Some learners may be more vulnerable online due to additional learning needs, disabilities, care experience, mental health needs, digital exclusion or other factors.

These differences will be considered when applying this policy, and reasonable adjustments or additional support will be provided where appropriate to help all learners engage safely with digital technologies.

This policy forms part of the Information Governance Framework and must be read and applied in conjunction with it.

3 Standards of Use and Behaviour

These requirements focus on safeguarding, behaviour and the prevention of harm in online activity, whether undertaken on College systems, personal devices or external platforms.

3.1 What You Must Do:

- act safely, respectfully and professionally online, whether activity is personal or College-related
- maintain appropriate professional boundaries when communicating online
- protect personal, sensitive, and confidential information
- use College-approved platforms (such as Teams or Canvas) for communication with learners and for teaching and learning activities – staff only
- ensure photographs, recordings or filming of learners or staff are authorised for College purposes and have an appropriate lawful basis

- store and share authorised images and recordings securely
- use artificial intelligence (AI) tools in ways that do not compromise safeguarding, data protection, wellbeing, academic integrity or assessment security, and in line with College guidance
- configure privacy settings on online platforms to reduce the risk of unauthorised access to, or disclosure of, personal information
- use digital communication tools (including email, messaging, and collaboration platforms) professionally and responsibly, recognising that communications sent through College ICT systems reflect on the organisation and may have safeguarding or professional implications
- exercise caution when opening attachments, following links or responding to unfamiliar senders
- report any safeguarding or online safety concerns promptly, including concerns about sexualised behaviour or image-based abuse
- report concerns even where incidents occur off-site, outside College hours or using personal devices
- report AI-generated content that raises safeguarding concerns through appropriate College channels

3.2 What You Must Not Do:

- engage in bullying, harassment or discriminatory behaviour online
- engage in cyberbullying, online sexual harassment, image-based abuse, peer-on-peer abuse or any form of coercive or exploitative online behaviour
- access, create or share illegal or harmful content
- participate in online activity that could bring the College into disrepute
- initiate or engage in direct social media connections or private messaging with learners outside approved College platforms
- use social media to communicate with learners about College matters outside approved College systems
- use the College name, branding or imagery on personal accounts in a way that implies College endorsement without authorisation
- disclose confidential, sensitive or personal information without appropriate authorisation
- upload personal or sensitive data to public AI tools unless explicitly approved and governed by an appropriate Data Protection Impact Assessment (DPIA)
- use AI tools that expose learners to unsafe or unmoderated content
- share usernames, passwords or authentication codes with others
- assume that email or online communications using College systems are fully private or exempt from monitoring required for safeguarding, security or legal purposes.

INFORMATION SECURITY POLICY

1 Policy Statement

The College is committed to protecting the confidentiality, integrity and availability of College ICT. Effective information security supports teaching and learning, enables efficient operations, and reduces operational, financial and reputational risk, while being applied in a proportionate and risk-based manner.

This policy supports compliance with Cyber Essentials and aligns with ISO/IEC 27001 principles.

2 Purpose and Scope

This policy sets the College's information security expectations and is supported by detailed standards, procedures and guidance within the Information Security Framework.

This policy aims to:

- protect College ICT from loss, misuse, unauthorised access or disruption
- reduce the likelihood and impact of information security incidents
- define expectations for secure behaviour and system use
- support safeguarding, privacy and online safety

This policy forms part of the Information Governance Framework and must be read and applied in conjunction with it.

3 Information Security Principles

The following principles underpin the College's approach to information security and are based on:

- privacy and safeguarding by design
- least privilege access
- defence in depth
- proportionate, risk-based controls
- shared responsibility
- continual review and improvement

Information security risks are identified, assessed and managed on an ongoing basis so that risks remain within acceptable limits.

4 Information Security Commitments

4.1 Information Asset Management

The College will manage its information and College ICT as information assets, ensuring clear ownership and appropriate protection throughout their lifecycle.

4.2 Information Classification

The College will classify its information to ensure it receives appropriate protection and will apply handling requirements that reflect the sensitivity, importance and use of that information.

4.3 Access Control and Authentication

The College will ensure that access to its systems and information is controlled, appropriate to users' roles, and managed securely throughout the lifecycle of user accounts. Appropriate authentication measures, including multi-factor authentication where available, will be used to protect access.

4.4 Device and Endpoint Security

The College will ensure that College-owned devices and endpoints are managed and protected appropriately to prevent unauthorised access, data loss or compromise, and to support the secure use, maintenance and disposal of equipment.

4.5 Network and Infrastructure Security

The College will ensure that its networks and supporting infrastructure are protected against unauthorised access, misuse and disruption, using appropriate technical and organisational controls to maintain security, resilience and reliability.

4.6 Information and Data Security

The College will ensure that information is stored, shared and disposed of securely, with appropriate protections applied to prevent unauthorised access, loss or disclosure, particularly where information is personal or sensitive.

4.7 Email, Phishing and User Awareness

The College will promote secure use of email and messaging systems through appropriate technical protections, user awareness and reporting arrangements, to reduce the risk of phishing, fraud and other social engineering threats.

4.8 Third-Party and Supplier Security

The College will manage information security risks arising from third-party and supplier relationships by applying appropriate controls, oversight and assurance throughout the lifecycle of those arrangements.

4.9 Backup, Resilience and Availability

The College will ensure that appropriate backup and recovery arrangements are in place to protect

critical systems and information and to support business continuity and operational resilience.

4.10 Incident Management

The College will ensure that information security incidents are identified, reported and managed promptly and proportionately, to reduce harm, restore services and prevent recurrence.

DATA PROTECTION POLICY

1 Policy Statement

The College is committed to protecting personal data and respecting the privacy of individuals. Effective data protection supports safeguarding, trust and confidence in how the College works with learners, staff, partners and the wider community.

The College will process personal data lawfully, fairly and transparently, in line with data protection law.

2 Purpose and Scope

This policy sets out the College's expectations for the lawful and responsible handling of personal data. It aims to:

- protect the rights and freedoms of individuals whose personal data the College processes
- ensure personal data is managed fairly, securely and transparently
- support safeguarding, privacy and information security across the organisation
- provide a consistent and accountable approach to data protection

This policy forms part of the Information Governance Framework and must be read and applied in conjunction with it.

3 Data Protection Principles

The following principles underpin the College's approach to handling personal data and guide how data protection decisions are made, and compliance is demonstrated under this policy.

The College will process personal data in accordance with the data protection principles. Personal data will be:

- processed lawfully, fairly and transparently
- collected for specified, explicit and legitimate purposes
- adequate, relevant and limited to what is necessary
- accurate and kept up to date
- retained only for as long as necessary
- protected through appropriate security measures

The College recognises its accountability for compliance with these principles. Evidence of compliance is maintained through governance arrangements, policies, procedures, records and training.

4 Data Protection Commitments

4.1 Lawful and Fair Processing

The College will ensure that all processing of personal data has a valid lawful basis and that individuals are informed about how their personal data is used through clear privacy and fair processing notices.

Arrangements are in place to support individuals' rights under data protection law, including access to their personal data. Requests relating to personal data are managed through processes overseen by the Data Protection Officer.

Data Protection Impact Assessments will be completed where processing is likely to result in an elevated risk to the rights and freedoms of individuals, including the introduction of new systems, technologies, or processing activities.

4.2 Information Security and Data Protection

The College will protect personal data through appropriate technical and organisational measures, aligned with the Information Security Policy and supporting standards.

Security controls are designed to prevent unauthorised access, loss, misuse or disclosure of personal data and to support confidentiality, integrity and availability. Data protection and information security are managed together as part of the College's overall risk management and safeguarding approach.

4.3 Data Sharing and Disclosure

The College will share personal data only where there is a valid lawful basis and where appropriate safeguards are in place.

Data sharing with third parties, including partners and contractors, will be governed by appropriate agreements and oversight arrangements to ensure personal data is protected and used only for authorised purposes.

Disclosures to external bodies, including public authorities, will be managed carefully and proportionately in accordance with College policy and applicable law.

4.4 Personal Data Breaches

The College will manage personal data breaches promptly and proportionately to reduce harm and to meet regulatory obligations. All suspected or actual personal data breaches must be reported immediately through the College's incident reporting arrangements.

Breaches involving personal data are assessed and managed with oversight from the Data Protection Officer, in line with the Information Security Incident process.

Where a breach is likely to result in a risk to the rights and freedoms of individuals, the College will notify the Information Commissioner's Office (ICO) without undue delay and, where feasible, within 72 hours of becoming aware of the breach.