Information Technology (IT) Acceptable Use and Information Security Policy

Policy no:	DIG 2.6
Version no. & date:	Version 3.4 - May 2026 (Draft)
Author:	Tiji Xavier
Policy Owner:	IT Manager
Last review date:	May 2026
Next review due:	May 2027
Responsible Committee:	Operations Committee
Approved by & date:	College Management Team – May 2026
External reference points:	UK GDPR Article 32; Data Protection Act 2018; Computer Misuse Act 1990; Freedom of Information Act 2000; Counterterrorism and Security Act 2015 (Prevent Duty); NCSC Cyber Essentials; NCSC 10 Steps to Cyber Security; ICO guidance on security of personal data; QAA Quality Code; OfS regulatory requirements
Linked policies:	DIG 2.1 Data Protection and Confidentiality Policy; DIG 2.4 Records Management and Data Retention Policy; DIG 2.5 Information Technology and Digital Resources Policy; Information Security Incident Response Procedure; Data Breach Procedure; Business Continuity and Crisis Management Procedures; Staff Code of Conduct; Student Conduct Policy; Employee Relations Policy
Audience:	All staff, students, contractors, temporary staff, third-party service providers, and authorised users of UKCBC IT systems

1. Purpose

The purpose of this policy is to define the acceptable use and information security requirements for information technology systems at the UK College of Business and Computing (UKCBC).

This policy aims to:

- protect UKCBC information systems and data from unauthorised access, misuse, loss, or damage
- ensure compliance with relevant legislation and regulatory requirements
- provide clear guidance to staff, students, and authorised users regarding the responsible use of IT systems
- support the secure delivery of teaching, learning, and administrative services
- define governance, accountability, escalation, and assurance expectations for information security and acceptable use

All users must comply with this policy and with security controls established by the College. Failure to comply may result in action in accordance with relevant College procedures.

2. Scope

This policy applies to all users of UKCBC IT systems and information assets, including:

- staff
- students
- contractors
- consultants
- temporary staff
- third-party service providers
- other authorised users of UKCBC systems

It covers the use of all IT resources owned, managed, operated, or authorised by UKCBC, including:

- computers and workstations
- servers and networks
- internet access
- email systems
- telephone and communication systems
- cloud services
- learning platforms
- student management systems
- portable devices
- remote access services
- institution-owned devices and personally owned devices where authorised for college use

This policy applies to on-site use, remote access, off-site working, and any authorised use of UKCBC information or systems from external locations.

3. External Reference Points

This policy has been developed with reference to relevant legislation, regulatory requirements, and recognised guidance on information security and acceptable use within the UK higher education sector.

Legislative Framework

This policy aligns with the following legislation and regulatory expectations:

- UK General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018
- Computer Misuse Act 1990
- Freedom of Information Act 2000
- Counter-Terrorism and Security Act 2015 (Prevent Duty)

The policy also supports sector expectations defined by:

- QAA Quality Code
- Office for Students (OfS) regulatory requirements

External Security Guidance

The policy has also been informed by recognised UK cyber security and information governance guidance including:

- National Cyber Security Centre (NCSC) guidance on cyber security governance
- NCSC 10 Steps to Cyber Security framework
- Cyber Essentials security principles
- Information Commissioner's Office (ICO) guidance on security of personal data
- UK GDPR Article 32 - Security of processing

Sector Alignment and Institutional Partnerships

UKCBC aligns its information technology governance practices with recognised standards within the UK higher education sector. The College considers relevant frameworks and guidance adopted by partner universities and sector regulators when developing its IT policies and procedures.

Where appropriate, reference is made to institutional governance approaches used by partner universities and sector bodies to ensure that UKCBC maintains secure, reliable, and compliant information technology systems supporting teaching, learning, and administration.

4. Institutional IT Systems

UKCBC operates several institutional IT systems which support academic delivery and administration. These include but are not limited to:

- Student Information System (SITS)
- Virtual Learning Environment (Moodle)
- Microsoft 365 collaboration platform
- network infrastructure and campus Wi-Fi
- administrative and financial systems
- email and communication platforms

These systems are managed through institutional governance arrangements and are subject to the principles and controls outlined in this policy and associated procedures.

Third-party and cloud-hosted systems used by UKCBC are subject to appropriate governance, contractual, data protection and security considerations. Where systems are provided or hosted by external suppliers, UKCBC will seek appropriate assurance regarding service availability, security obligations, data handling,

data residency where applicable, and compliance with relevant legal and regulatory requirements. Supplier and third-party service arrangements are managed in accordance with applicable procurement, data protection and information security requirements.

5. Key Definitions

Information Asset
Any information, data, system, device, record, platform, or service that supports the operations, teaching, research, administration, or governance of UKCBC.

Information Security
The protection of information and information systems to ensure their confidentiality, integrity, and availability.

Acceptable Use
The use of UKCBC information systems and resources in a responsible, lawful, authorised, and proportionate manner consistent with institutional policies.

User
Any individual authorised to access UKCBC systems, including staff, students, contractors, temporary staff, and third-party service providers.

Personal Data
Information relating to an identified or identifiable individual as defined under the UK General Data Protection Regulation (UK GDPR).

Information Security Incident
Any actual or suspected event that may compromise the confidentiality, integrity, or availability of UKCBC information systems, information assets, or data.

Major Incident
An incident that has, or may have, a significant impact on college operations, information assets, legal obligations, reputation, or continuity of teaching and administration.

6. Acceptable Use of IT Systems

UKCBC IT systems are provided primarily for the purposes of:

- teaching and learning
- research activities
- administrative operations
- official College communication

Limited personal use may be permitted provided that such use:

- does not interfere with work or academic responsibilities
- does not consume excessive system resources
- does not breach College policies, contractual obligations, or legal requirements

Personal use must remain incidental and must not create security, legal, operational, or reputational risks for the College.

Users must ensure that their use of IT systems is responsible, lawful, and consistent with the values and reputation of the College.

Users must also ensure that their use of UKCBC IT systems does not compromise the security, integrity, availability, or reputation of the College.

7. Information Security Principles

UKCBC manages information security in accordance with the following principles:

- information must be protected in terms of confidentiality, integrity, and availability
- security controls should follow a risk-based approach appropriate to the sensitivity and value of the information being protected
- access to systems and information should follow the principle of least privilege, ensuring that users only have access necessary to perform their roles
- information must be handled securely throughout its lifecycle, including creation, storage, transmission, retention, archiving, and disposal
- security controls must be monitored and reviewed regularly
- security incidents must be managed in accordance with defined response procedures
- all users share responsibility for maintaining the security of UKCBC systems and information assets

8. Information Security Controls

UKCBC is committed to protecting its information assets from threats including unauthorised access, misuse, loss, disruption, or disclosure.

The College will implement appropriate technical and organisational security measures to safeguard its systems and information in accordance with recognised cyber security guidance, legal obligations, and regulatory requirements.

Controls may include access management, user authentication, device management, secure configuration, backup, resilience, monitoring, incident management, and user awareness measures. Detailed technical configurations and operational procedures are maintained separately in supporting standards and procedures.

All users are expected to follow institutional security practices and guidance issued by IT Services to support the protection of information assets.

Supporting technical security standards and operational procedures are maintained by IT Services and are available to relevant staff on request or through the appropriate internal guidance channels.

9. User Responsibilities

All users must:

- protect their login credentials and passwords
- lock or log out of devices when unattended
- ensure confidential and restricted information is handled securely
- comply with security guidance and controls issued by IT Services
- report suspected information security incidents promptly via the designated reporting channel

Users must not:

- share login credentials
- access data or systems without authorisation
- attempt to bypass security controls

- install unauthorised software
- connect unauthorised devices to the network
- store College data on unauthorised devices or external storage
- use UKCBC systems in a way that creates security, legal, safeguarding, operational, or reputational risk

  Authorised devices and approved storage locations are defined by IT Services and may include College-managed devices, approved cloud platforms, and other systems formally authorised for college use. Users should seek guidance from IT Services where they are unsure whether a device, storage location, or digital service is approved.

10. Information Classification

UKCBC information assets are classified according to sensitivity and impact if disclosed, altered, lost, or made unavailable.

Classification	Description	Examples
Public	Information approved for public release	marketing material; published policies
Internal	Operational information for internal use	internal procedures; internal announcements
Confidential	Sensitive institutional or personal data	student records; HR records; non-public management information
Restricted	Highly sensitive information requiring strict control	disciplinary cases; financial records; sensitive investigations

Handling, storage, transmission, retention, and disposal of information must align with its classification level and associated security controls.

11. Data Protection and Confidentiality

Users who have access to personal or confidential data must ensure that such information:

- is accessed only where necessary and authorised
- is stored securely
- is not disclosed to unauthorised persons
- is processed in accordance with UK GDPR, the Data Protection Act 2018, and DIG 2.1 Data Protection and Confidentiality Policy

Sensitive information must not be stored on personal devices or removable media without authorisation. Data protection principles, lawful processing requirements, and individual rights are defined in the College's data protection policies and procedures.

12. Remote Access and Devices

Where remote access is authorised, users must use approved routes and follow College guidance for secure access to systems and information.

Guidance on what constitutes an appropriately secured device is provided by IT Services. Users must follow College guidance when accessing UKCBC systems remotely or from personal devices.

Only College-approved devices or securely configured personal devices may be used to access College systems where authorised.

Users must ensure that devices used to access UKCBC systems are appropriately secured, maintained, and protected from unauthorised access.

Portable devices such as laptops and storage media must be kept secure at all times. Loss or suspected compromise of any device used to access College systems must be reported promptly.

13. Internet and Email Use

Internet and email services are provided for academic and operational purposes. Users must use these services responsibly and in accordance with college policies and legal requirements.

Users must not use College systems to:

- access illegal or inappropriate content
- distribute offensive, defamatory, discriminatory, harassing, or extremist material
- conduct unauthorised commercial activities
- distribute malware or harmful software
- send or store College information in a way that creates security, legal, safeguarding, or reputational risk

Downloading software, files, or digital materials must comply with licensing arrangements, copyright requirements, and approval processes where applicable.

Use of Artificial Intelligence and Generative AI Tools

Users must use artificial intelligence and generative AI tools, including services such as ChatGPT, Microsoft Copilot and similar platforms, in a responsible and lawful manner.

Users must not upload, enter, or process confidential College information, personal data, student records, commercially sensitive information, assessment materials, or unpublished institutional documents into external AI tools unless the tool has been approved for that purpose by the College.

Where AI tools are used to support academic, administrative, or operational activities, users remain responsible for verifying the accuracy, appropriateness, and integrity of any output before it is used or shared.

Use of AI tools must comply with applicable College policies, including data protection, academic integrity, information security, and acceptable use requirements.

14. Monitoring, Logging and Assurance

UKCBC reserves the right to monitor the use of its IT systems for purposes including maintaining system security, investigating suspected misuse, ensuring operational performance, and meeting legal and regulatory obligations.

Monitoring may include analysis of network activity, system access logs, internet usage, and email traffic.

Monitoring is conducted in a proportionate and lawful manner and is limited to what is necessary to meet security, operational, safeguarding, and legal requirements.

Compliance with this policy may be reviewed through appropriate assurance activities, including audits, management reviews, incident analysis, access reviews, and risk assessments.

Monitoring will be conducted transparently, proportionately and in accordance with applicable data protection requirements. Further information on how personal data may be processed for monitoring, security and operational purposes is set out in the College's Data Protection and Confidentiality Policy and relevant privacy notices.

15. Prevent Duty and Safeguarding

UKCBC complies with its obligations under the Prevent Duty and safeguarding requirements.

IT systems may implement filtering and monitoring technologies to restrict access to online material promoting extremism, radicalisation, terrorism, or other harmful content.

Any suspected misuse may be addressed through the College's relevant safeguarding and conduct procedures and may be escalated where required.

16. Incident Reporting and Escalation

Users must immediately report any suspected or actual information security incident to IT Services through the designated reporting route, such as the IT helpdesk or other College-approved reporting channel.

Examples include:

- suspected hacking attempts
- malware infections
- lost or stolen devices
- accidental disclosure of confidential information
- unauthorised access to systems or information
- suspected phishing, compromised accounts, or suspicious email activity

Contact details for reporting IT incidents are made available through internal College communication channels, including the intranet or staff guidance where applicable.

IT Services will assess reported incidents and escalate significant risks, breaches, or control failures in accordance with institutional governance arrangements.

Major incidents are managed in accordance with the College's Incident Response, Data Breach, Business Continuity, and Crisis Management procedures, as applicable.

Failure to report suspected incidents promptly may increase risk to the organisation and may be considered under relevant staff or student procedures.

17. Risk Management

Information security risks are identified, assessed, and managed in accordance with the College's risk management framework.

Significant information security risks, incidents, or control weaknesses must be recorded, reviewed, and escalated through appropriate governance routes.

Risk treatment actions may include changes to controls, user guidance, training, system configuration, supplier management, or business continuity arrangements.

18. Compliance and Breaches

All users are expected to comply with this policy and with any associated procedures, controls, or guidance issued by the College.

Non-compliance with this policy may result in action in accordance with the College's staff or student conduct procedures and, where applicable, legal consequences.

Where breaches involve personal data, safeguarding concerns, criminal activity, or significant operational risk, they will be escalated in accordance with the relevant College procedures and governance arrangements.

19. Roles and Responsibilities

Operations Committee

Provides oversight of this policy, reviews significant issues or risks, and ensures that information security and acceptable use are considered within institutional governance.

Executive Leadership Team

Receives escalation of significant information security risks, incidents, control failures, or matters with potential strategic, legal, regulatory, operational, or reputational impact.

IT Manager

Responsible for the operational management of information security controls and for supporting implementation of this policy across college systems.

IT Services

Responsible for supporting the secure operation of UKCBC information systems, implementing institutional information security measures, responding to reported incidents, and supporting compliance monitoring.

People and Culture

Responsible for supporting staff awareness and training arrangements relating to information security, acceptable use, and relevant staff policy obligations.

Department Heads and Line Managers

Responsible for promoting compliance with this policy within their areas, ensuring staff understand relevant expectations, and escalating concerns where required.

Staff, Students and Authorised Users

Responsible for complying with this policy, protecting access credentials, using systems responsibly, following College guidance, and reporting security concerns promptly.

20. Governance and Escalation

The IT Manager is responsible for the operational management of information security controls within the College.

Oversight of information security is provided through the Operations Committee. Significant risks, incidents, or control failures are escalated to the Executive Leadership Team in accordance with the College's governance framework.

Information security risks are identified, assessed, and managed in accordance with the College's risk management framework. Where required, actions are tracked through appropriate management and committee reporting routes.

21. Policy Impact and Implementation Expectations

This policy requires staff, students, contractors, and authorised users to follow College requirements for secure and responsible use of systems and information.

Implementation of this policy is supported through staff guidance, user communications, and appropriate information security awareness activities. Staff may be required to complete information security or acceptable use training as determined by the College. Training and awareness activities will be reviewed periodically to support compliance with this policy and recognised cyber security guidance.

Implementation of this policy may require supporting actions such as user communication, training, access reviews, monitoring, incident reporting arrangements, and periodic compliance checks.

Departments must cooperate with IT Services, People and Culture, and relevant governance bodies to ensure that policy expectations are understood and applied in practice.

22. Policy Boundaries

This policy defines institutional expectations for information security and acceptable use of UKCBC systems.

It does not:

- specify detailed technical security configurations or system settings
- define lawful processing of personal data, which is covered by DIG 2.1 Data Protection and Confidentiality Policy
- define records retention requirements, which are covered by DIG 2.4 Records Management and Data Retention Policy
- define IT infrastructure strategy or procurement decisions, which are covered by DIG 2.5 Information Technology and Digital Resources Policy
- define detailed incident response steps, which are covered by the Information Security Incident Response Procedure and Data Breach Procedure
- define crisis management or business continuity processes, which are covered by the College's Business Continuity and Crisis Management procedures
- define disciplinary processes, which are covered by Employee Relations, Staff Conduct, and Student Conduct policies

Operational procedures, technical standards, implementation guidance, training materials, and detailed response plans are maintained separately and version controlled where required.

23. Policy Review

This policy will be reviewed annually, or earlier where required due to significant changes in legislation, regulation, institutional systems, risk profile, security incidents, or sector guidance.

The review will consider:

- regulatory requirements
- emerging cybersecurity risks
- technological developments
- sector best practice
- incident trends and audit findings
- changes to institutional systems or governance arrangements