Information Technology and Digital Resources Policy

Policy no:	DIG 2.5
Version no. & date:	Version 1.1 - April 2026
Author:	Tiji Xavier
Policy Owner:	IT Manager
Last review date:	April 2026
Next review due:	April 2027
Responsible Committee:	Operations Committee
Approved by & date:	College Management Team – May 2026
External reference points:	Office for Students regulatory framework; QAA Quality Code; UK GDPR; Data Protection Act 2018; Freedom of Information Act 2000; NCSC guidance; Jisc digital infrastructure and learning technology guidance where applicable
Linked policies:	DIG 2.1 Data Protection and Confidentiality Policy; DIG 2.4 Records Management and Data Retention Policy; DIG 2.6 Information Security and Acceptable Use Policy; Information Security Incident Response Procedure; Business Continuity / Crisis Management Procedures; Procurement and Financial Regulations; Staff and Student Conduct Policies
Audience:	All staff, students, contractors, third-party service providers, and authorised users of UKCBC IT systems and digital resources

1. Purpose

The purpose of this policy is to define how UKCBC governs, manages, maintains and utilises its information technology systems and digital resources to support teaching, learning, research, administration and institutional operations.

This policy aims to:

- ensure the effective, reliable and sustainable provision of IT services across the College
- support the delivery of high-quality digital learning, assessment and administrative services
- define governance arrangements for IT infrastructure, digital platforms and technology-enabled services
- ensure that technology decisions align with regulatory, academic, operational and financial requirements
- promote responsible planning, procurement, lifecycle management and review of IT resources
- support continuity, resilience and risk management for key institutional systems.

2. Scope

This policy applies to all UKCBC information technology infrastructure, systems, services and digital resources owned, managed, procured or used by the College.

It applies to:

- staff
- students
- contractors
- consultants
- temporary staff
- third-party service providers
- authorised users of UKCBC IT services.

It covers, but is not limited to:

- network infrastructure and connectivity
- servers, hosting environments and cloud platforms
- teaching, learning and assessment systems
- student information and administrative systems
- communication and collaboration tools
- IT support and service management arrangements
- procurement, approval and lifecycle management of digital resources.

3. External Reference Points

This policy has been developed with reference to relevant legislation, regulatory expectations and recognised sector guidance relating to information technology governance, digital resources and the delivery of technology-enabled education.

3.1 Legislative and Regulatory Framework

This policy has been developed with reference to the following legislation and regulatory expectations:

- UK General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018
- Freedom of Information Act 2000
- Computer Misuse Act 1990, where relevant
- Counter-Terrorism and Security Act 2015, where relevant
- Public Sector Bodies (Websites and Mobile Applications) (No. 2) Accessibility Regulations 2018, where applicable

3.2 Sector Guidance

- Office for Students (OfS) regulatory requirements
- QAA Quality Code
- National Cyber Security Centre (NCSC) guidance, where relevant to secure operation of IT services
- Jisc guidance and resources relating to digital infrastructure, connectivity and learning technologies, where applicable.

3.3 Sector Alignment and Institutional Partnerships

UKCBC aligns its IT governance practices with recognised standards within the UK higher education sector. The College considers relevant frameworks and guidance adopted by partner universities, sector bodies and regulators when developing, reviewing and improving its IT systems and digital resources.

4. Policy Statement

UKCBC is committed to providing reliable, secure, accessible and effective information technology services that support the College's academic and operational objectives.

The College will ensure that IT infrastructure and digital resources are:

- fit for purpose and aligned with institutional priorities
- appropriately governed, supported and maintained
- accessible to authorised users, subject to role and operational requirements
- procured and managed in accordance with approved processes
- reviewed for performance, value, resilience and risk

- supported by appropriate continuity, recovery and escalation arrangements.

5. Key Definitions

For the purposes of this policy, the following definitions apply.

Term	Definition
IT Infrastructure	The hardware, software, networks, servers, cloud services and technical environments that support UKCBC operations.
Digital Resources	Technology-enabled systems, platforms, tools and services used to support teaching, learning, administration, communication or institutional management.
Institutional System	A core system used to deliver or manage College operations, such as SITS, Moodle, Office 365 or other approved business systems.
System Owner	The person or function accountable for the business use, governance and suitability of a system.
Service Owner	The person or function responsible for coordinating the delivery and support of an IT service.
Lifecycle Management	The planning, procurement, deployment, review, maintenance and retirement of IT systems and digital resources.
Authorised User	An individual who has been granted permission to access UKCBC IT systems or digital resources.

6. Institutional IT and Digital Resources

UKCBC operates a range of IT systems and digital platforms to support teaching, learning, administration and institutional management. These include, but are not limited to:

- Student Information System (SITS)
- Virtual Learning Environment (Moodle)
- Microsoft 365 collaboration platform
- network infrastructure and Wi-Fi services
- administrative and finance systems
- communication and collaboration tools
- digital learning and assessment platforms.

These systems are managed through appropriate institutional governance arrangements and must be used in accordance with linked policies, procedures and approved operational guidance.

7. IT Governance Principles

UKCBC manages IT systems and digital resources in accordance with the following principles:

- IT services must support the strategic, academic and operational objectives of the College.
- Systems must be reliable, available, appropriately supported and reviewed against institutional need.
- Digital resources must be accessible and usable by authorised users, subject to role, system and security requirements.

- IT investments must be planned, justified, approved and aligned with institutional priorities.
- Risks associated with IT systems and digital resources must be identified, assessed, managed and escalated through appropriate governance arrangements.
- Technology decisions should consider sustainability, value for money, interoperability and long-term support requirements.

8. Governance, Accountability and Escalation

The IT Manager is responsible for the operational management of IT systems, infrastructure and digital resources within the scope of this policy.

Oversight of IT governance is provided through the Operations Committee. Significant technology risks, service failures, control weaknesses, major incidents or investment decisions are escalated to the Executive Leadership Team in accordance with the College's governance framework.

Department Heads and system owners are responsible for ensuring that IT systems and digital resources used within their areas remain appropriate, supported and aligned with college policies.

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

9. Management of IT Infrastructure

UKCBC will manage its IT infrastructure to support effective institutional operations and the delivery of teaching and learning.

The College will ensure that IT infrastructure:

- supports operational and academic requirements
- provides appropriate performance, availability and capacity
- is monitored and reviewed to identify risks and improvement needs
- is maintained and upgraded where necessary through approved planning processes
- supports authorised on-site and remote access arrangements
- is documented at an appropriate level to support continuity, support and accountability.

Detailed technical configurations are maintained separately in supporting procedures, standards and operational documentation.

10. Digital Learning and Academic Systems

UKCBC will provide and maintain digital platforms that support teaching, learning, assessment, communication, and academic administration.

Digital learning and academic systems must:

- support effective delivery of academic programmes

- be accessible to students and staff
- support communication, collaboration, assessment, feedback, and learning activities
- be reviewed periodically to ensure they remain fit for purpose
- be managed in a way that supports student experience and operational continuity
- align with accessibility expectations set out in this policy
- be subject to appropriate governance where AI-enabled or emerging technology features are introduced.

Students and staff can expect core academic systems to be managed with appropriate consideration for availability, accessibility, usability, and support. Planned maintenance or significant service changes should be communicated to affected users where practicable.

Academic systems are governed collaboratively between IT Services, academic leadership, and relevant professional services teams to ensure alignment with curriculum delivery, student experience, and institutional requirements.

11. Procurement and Approval of Digital Resources

All new IT systems, digital platforms, software or technology-enabled services must be approved through appropriate governance and procurement processes before being introduced.

Approval should consider:

- business need and alignment with institutional priorities
- cost, value for money and ongoing resource implications
- compatibility with existing systems and data flows
- information security and data protection requirements
- accessibility and usability considerations
- supplier support, contractual terms and exit arrangements
- business continuity and resilience implications.

All proposed IT systems, cloud services, digital learning tools, AI-enabled platforms, and externally hosted services must undergo appropriate due diligence before approval. This may include consideration of information security, data protection, accessibility, contractual terms, supplier assurance, compatibility with existing systems, support requirements, and operational risk.

The use of unauthorised systems, applications, cloud services, or digital tools outside approved governance arrangements, commonly referred to as “shadow IT”, is not permitted where it creates security, data protection, contractual, operational, or reputational risk to the College.

Where unauthorised systems or services are identified, they may be reviewed by IT Services and escalated through the appropriate governance or conduct procedures where necessary.

Unauthorised systems, applications or digital services must not be introduced for institutional use without approval.

12. Use of AI-Enabled and Emerging Technologies

AI-enabled systems, generative AI tools, automation platforms, and emerging digital technologies must be introduced through appropriate governance and approval processes.

Such tools must be assessed for data protection, information security, academic integrity, accessibility, contractual risk, transparency, and operational impact before being adopted for college use.

Users must not independently introduce AI-enabled tools or services for college business or academic delivery where this may involve College data, personal data, student information, assessment content, or institutional records without appropriate approval.

13. Lifecycle Management and Review

UKCBC will manage IT systems and digital resources throughout their lifecycle, from planning and procurement through to review, replacement or retirement.

Lifecycle management should include:

- identification of business and academic requirements
- approval and implementation planning
- periodic review of performance, usage and continuing need
- assessment of supportability, supplier risk and cost
- planned replacement, upgrade or retirement where systems no longer meet requirements.

14. Accessibility, Inclusion and Digital User Experience

UKCBC will seek to ensure that digital systems and services are accessible, inclusive, and usable by students, staff, and authorised users, in line with applicable legal, regulatory, and sector expectations.

Public-facing websites, mobile applications, and relevant digital services must be managed with regard to applicable accessibility requirements, including the Public Sector Bodies (Websites and Mobile Applications) (No. 2) Accessibility Regulations 2018 where applicable.

Accessibility, inclusion, and digital user experience should be considered when procuring, developing, reviewing, or significantly changing digital systems and services.

15. IT Service Provision and Support

UKCBC will provide IT support services to assist users in accessing and using institutional systems effectively.

IT service provision may include:

- user support and advice
- incident and request handling
- service monitoring and maintenance
- system access support
- coordination with suppliers and service providers
- communication of planned maintenance or service disruption where appropriate.

Users are expected to follow guidance issued by IT Services and to report faults, service issues or concerns through designated support channels.

16. Third-Party Systems and Supplier Management

Before onboarding third-party systems or suppliers, UKCBC will undertake proportionate due diligence to assess security, data protection, accessibility, service reliability, contractual obligations, and operational risks.

Where third-party systems process personal data on behalf of UKCBC, supplier arrangements must comply with applicable UK GDPR requirements, including appropriate controller/processor terms and consideration of sub-processor arrangements where relevant.

Data protection obligations relating to third-party systems and supplier contracts are addressed in DIG 2.1 Data Protection and Confidentiality Policy.

17. Data, System Ownership and Integration

Core institutional systems should have an identified business owner or responsible function. System ownership supports accountability for use, data quality, access requirements, process alignment and ongoing suitability.

System integrations and data flows must be managed in accordance with relevant data protection, information security, records management and operational requirements. This policy does not define lawful processing obligations, which are covered in DIG 2.1 Data Protection and Confidentiality Policy.

18. Business Continuity, Resilience and Crisis Management

UKCBC will take appropriate measures to support the continuity and resilience of key IT services and digital resources.

The College will seek to ensure that priority IT services can be restored in a timely manner following disruption, subject to the nature and severity of the incident.

Major incidents, significant service failures or crisis events involving IT systems are managed in accordance with the College's Incident Response, Business Continuity and Crisis Management procedures.

Priority IT systems and digital services should have defined recovery expectations appropriate to their institutional importance. Recovery priorities, including recovery time and recovery point expectations where applicable, are documented in business continuity, disaster recovery, or operational resilience procedures.

19. Monitoring, Assurance and Review of IT Services

IT systems and services will be monitored and reviewed to support performance, reliability, risk management and continuous improvement.

Monitoring and assurance may include:

- review of system availability and service performance
- assessment of incident and request trends
- review of system usage and continuing need
- risk assessment of key systems and suppliers
- review of planned improvements, upgrades and lifecycle requirements.

Monitoring will be conducted in accordance with relevant legal, data protection and institutional requirements.

20. Roles and Responsibilities

Role	Responsibility
Executive Leadership Team	Provides strategic oversight of significant IT risks, major technology decisions, resource priorities and escalated incidents.
Operations Committee	Provides governance oversight of IT operations, digital resources, service improvement, risk and resilience matters.
IT Manager	Responsible for operational management of IT infrastructure, IT services and digital resources within the scope of this policy.
IT Services	Supports the secure and effective operation of IT systems, service provision, supplier coordination, system maintenance and user support.
System Owners / Service Owners	Responsible for ensuring assigned systems or services remain appropriate for institutional use and are managed in line with relevant policies.
Department Heads	Responsible for ensuring that IT systems and digital resources used within their areas are approved, appropriate and used in accordance with policy.
People and Culture	Supports relevant staff training and awareness relating to institutional systems, digital working practices and linked policies where applicable.
Staff and Students	Responsible for using IT systems and digital resources appropriately, following institutional guidance and reporting issues or concerns.

21. Compliance and Breaches

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

Non-compliance may create operational, financial, legal, reputational or security risks and may be addressed through relevant institutional procedures, including staff or student conduct procedures where appropriate.

22. Policy Boundaries

This policy defines the governance and management of IT systems and digital resources.

It does not:

- define information security or acceptable use expectations, which are covered by DIG 2.6 Information Security and Acceptable Use Policy
- 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 detailed technical configurations, operational procedures or system settings
- replace procurement, finance, staff conduct, student conduct or crisis management procedures.

Operational procedures, technical standards, implementation guidance and system-level documentation are maintained separately.

23. Policy Review

This policy will be reviewed annually, or sooner, where significant changes occur, to ensure alignment with institutional priorities, regulatory expectations, technological developments, risk management requirements and sector practice.