Data Protection and Confidentiality Policy

Policy no:	DIG 2.1
Version no. & date:	Version 6.0 – May 2026
Author:	Pauline Williams
Policy Owner:	Director of Governance Quality and Student Success
Last review date:	January 2026
Next review due:	May 2028
Responsible Committee:	Operations Committee
Approved by & date:	College Management Team – May 2026
External reference points:	UK General Data Protection Regulation (UK GDPR) Data Protection Act 2018 (DPA 2018) Privacy and Electronic Communications Regulations 2003 (PECR) Data (Use and Access) Act 2025 UAE Personal Data Protection Law (Federal Decree-Law No. 45 of 2021) (UAE PDPL) Information Commissioner's Office (ICO) guidance and codes of practice
Linked policies:	DIG 2.3 Student Privacy Notice; DIG 2.4 Records Management and Data Retention Policy; DIG 2.6 Information Security and Acceptable Use Policy; DIG 2.7 Subject Access Request and Individual Data Rights Policy; HSE 4.4 Cookie Policy; SLCC 6.1 Terms and Conditions; SLCC 6.12 Admissions Policy and Procedure
Audience:	All staff, students, prospects, applicants, alumni, contractors and third-party data processors

1. Purpose

This policy sets out how UK College of Business and Computing (UKCBC or the College) collects, uses, stores, shares and protects personal data across all its operations and in all jurisdictions in which it operates. It establishes the framework within which the College meets its obligations under data protection law and ensures that all data subjects, including staff, students, prospects, applicants, alumni, contractors and third parties, can understand how their personal data is handled and what rights they hold.

The College is registered with the Information Commissioner's Office (ICO) as a data controller. Where the College operates outside the UK, including at its Dubai campus, it applies the equivalent obligations under applicable local data protection law.

2. Scope

This policy applies to all personal data processed by the College in connection with its operations, regardless of the format in which that data is held (electronic, paper or otherwise) and regardless of the location of storage or the ownership of the equipment used.

This policy applies to:

- all staff, including employees, contractors, agency workers and volunteers
- all students, including prospects, applicants, enrolled students, students on deferral or interruption, and alumni
- all authorised third-party processors acting on behalf of the College.

This policy covers personal data held at all stages of the staff and student lifecycle, from initial engagement through to the end of the applicable retention period.

3. Definitions

The following definitions apply throughout this policy:

- **Personal Data:** Information that relates to an identified or identifiable living individual. This includes data held in any form that can be processed automatically or within a structured manual filing system and encompasses factual statements, expressions of opinion, photographs, video recordings and audio recordings.

- **Data Subject:** The identified or identifiable living individual to whom personal data relates.
- **Data Controller:** The organisation that determines the purposes and means of processing personal data. UKCBC acts as data controller for personal data covered by this policy.
- **Data Processor:** A third-party organisation or individual that processes personal data on behalf of the College as data controller.
- **Data User:** An authorised member of staff or student who accesses personal data held by the College in the course of their duties or studies.
- **Processing:** Any operation performed on personal data, including collection, recording, organisation, storage, adaptation, retrieval, use, disclosure, erasure or destruction.
- **Special Category Personal Data:** Personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data, data concerning health, or data concerning an individual's sex life or sexual orientation. This data attracts additional protections under Article 9 UK GDPR.
- **Criminal Convictions and Offences Data:** Personal data relating to criminal convictions, offences or related security measures. This data is subject to separate protections under Article 10 UK GDPR and must only be processed under official authority or with specific legal authorisation. It is distinct from Special Category Data and must be treated accordingly.
- **Data Protection Impact Assessment (DPIA):** A structured process for identifying and mitigating the privacy risks of a new or changed processing activity.
- **International Data Transfer Agreement (IDTA):** The mechanism approved by the ICO for transferring personal data from the UK to third countries that do not benefit from an adequacy decision.

4. Roles and Responsibilities

4.1 Data Protection Officer

The College appoints a Data Protection Officer (DPO) who possesses sufficient knowledge and seniority to fulfil the role effectively. The DPO must operate with the degree of independence required by Article 38(6) UK GDPR and must not hold responsibilities that give rise to a conflict of interest with the data protection function. The College reviews this requirement as part of its annual governance assurance process.

The DPO is responsible for:

- promoting compliance with this policy and providing guidance to staff
- ensuring staff, students, contractors and volunteers are aware of their data protection obligations
- maintaining the College's registration with the ICO
- overseeing the handling of data subject rights requests in accordance with DIG 2.7
- leading on data breach assessment, notification and recording
- conducting periodic compliance audits
- advising on DPIAs and reviewing outcomes

The DPO has access to all documents relevant to the College's legal compliance under data protection legislation. The DPO can be contacted at: dpo@ukcbc.ac.uk

Where the College operates in jurisdictions outside the UK, it appoints a local data protection representative to provide local expertise and ensure compliance with applicable local law.

4.2 Data Policy Oversight Group

The College maintains a Data Policy Oversight Group, chaired by the Director of Governance Quality and Student Success, to oversee information and data governance across the institution. The Group works with the DPO to:

- review and approve data protection guidance and procedures
- oversee compliance audit activity and ICO registration
- ensure appropriate processes are in place for data subjects to exercise their rights
- review the Data Breach Log periodically

4.3 Heads of Department

Heads of Department are responsible for ensuring compliance with this policy within their areas. They must:

- ensure all new staff receive data protection induction training
- ensure staff receive regular refresher training

- ensure any profiling activity under their oversight is regularly reviewed for accuracy and appropriateness.

4.4 Head of People and Culture

The Head of People and Culture must:

- notify relevant departments, including IT Services and the Systems Team, promptly when staff join or leave the College, to ensure access to personal data is granted or withdrawn without delay
- ensure data protection training is available to all staff and records of completion are maintained
- maintain training records for staff at third-party processors carrying out activities on behalf of the College.

4.5 Head of IT and Systems

The Head of IT and Systems must ensure that all systems holding or processing personal data:

- are protected from unauthorised access to the best of the College's capabilities
- are kept up to date with respect to operating systems and security patches
- have suitable access controls and password policies in place
- can remove access for leavers and grant appropriate access to new staff.

4.6 Staff Responsibilities

Every member of staff has a personal responsibility to comply with this policy and with data protection legislation. Staff must:

- keep all personal data entrusted to them in the course of their work secure
- not disclose personal data, verbally or in writing, deliberately or accidentally, to any unauthorised party
- access personal data only for legitimate College business purposes
- not keep copies of personal data on portable devices or outside the College's authorised systems
- immediately alert their line manager or the DPO if they have or observe inappropriate access to personal data

- not share passwords or other means of access to personal data
- ensure that personal information they provide to the College is accurate and up to date
- where supervising students conducting work that involves personal data, ensure those students understand data protection obligations

Staff who are unsure whether a disclosure is authorised must seek advice from their line manager or the DPO before disclosing. Any unauthorised disclosure of personal data constitutes a breach of this policy and may constitute gross misconduct or a criminal offence.

4.7 Student Responsibilities

Students must inform the College promptly of any changes to their personal information. Where a student's coursework or project involves the processing of personal data, they must comply with data protection principles and obtain any necessary consent. Students should seek guidance from their supervisor or the DPO if they are uncertain of their obligations.

5. Data Protection Principles

As data controller, the College processes all personal data in accordance with the following principles, as set out in Article 5 UK GDPR:

5.1 Lawfulness, Fairness and Transparency

The College processes personal data lawfully, fairly and transparently. The College informs data subjects about how their data is used and ensures a lawful basis exists for all processing.

5.2 Purpose Limitation

The College collects personal data only for specified, explicit and legitimate purposes and does not process it in any manner incompatible with those purposes.

5.3 Data Minimisation

The College ensures that personal data collected and processed is adequate, relevant and limited to what is necessary for the purpose for which it is processed.

5.4 Accuracy

The College takes reasonable steps to ensure that personal data is accurate and, where necessary, kept up to date. Inaccurate data is erased or rectified without delay.

5.5 Storage Limitation

The College does not retain personal data for longer than is necessary for the purposes for which it was collected. Retention periods are set out in the Records Management and Data Retention Policy (DIG 2.4) and summarised in section 11 of this policy.

5.6 Integrity and Confidentiality

The College processes personal data securely using appropriate technical and organisational measures. These protect against unauthorised or unlawful processing and against accidental loss, destruction or damage.

5.7 Accountability

The College takes responsibility for compliance with data protection principles and demonstrates that compliance through policies, procedures, training records, audit trails and DPIAs.

6. Personal Data the College Collects

6.1 Staff and Contractor Data

The College collects and processes the following categories of personal data in respect of staff and contractors:

- contact and identity information, including name, address, telephone number and email address
- employment information, including contract details, job title, department and line management
- payroll, pension and financial information
- qualifications, training records and professional development information
- performance, conduct and disciplinary records

- leave, attendance and absence records
- health and wellbeing information where relevant to occupational health or reasonable adjustments
- equal opportunities monitoring data, provided voluntarily
- right to work documentation and immigration status where applicable
- CCTV footage recorded on College premises

6.2 Student, Prospect and Applicant Data

The College collects and processes the following categories of personal data throughout the student lifecycle, from initial enquiry to the end of the applicable retention period:

- contact and identity information, including name, date of birth, address and previous names
- application and enrolment information, including references, qualifications and supporting documentation
- biographical and diversity information, including ethnicity, nationality, gender identity and religious belief, where collected for statutory reporting or support purposes
- academic progress information, including attendance, assessment submissions, marks, feedback and records of deferrals, complaints or appeals
- communications via the student portal, email or written correspondence
- health, wellbeing, safeguarding and conduct information, where relevant to a duty of care or formal process
- immigration and visa information, where required to verify the right to study
- criminal convictions and offences data, where disclosed voluntarily during the application process; held separately under additional legal protections
- financial information, including bank details for payments, refunds or support funds, held securely on the finance system only
- technical information including IP addresses and device data collected automatically through the College's online systems
- CCTV footage recorded on College premises

Data is collected through direct interaction with the College's secure systems, through forms completed by or on behalf of the individual, or through data entry by authorised staff into systems

including the student management system, virtual learning environment, library system and finance system.

7. Lawful Basis for Processing

7.1 General Processing

The College processes personal data only where at least one of the following lawful bases applies under Article 6 UK GDPR:

- Consent: the data subject has given clear consent to processing for a specific purpose
- Contract: processing is necessary to fulfil a contract with the data subject or to take steps at their request before entering into one
- Legal obligation: processing is necessary for the College to comply with the law
- Vital interests: processing is necessary to protect someone's life
- Public task: processing is necessary to perform a task in the public interest or in the exercise of official functions with a clear basis in law
- Legitimate interests: processing is necessary for the College's legitimate interests or those of a third party, provided those interests are not overridden by the data subject's rights

Some processing of personal data is necessary for the College to fulfil its legal obligations, safeguarding duties and contractual responsibilities. Such processing does not rely on consent, and individuals cannot opt out of it without affecting the College's ability to deliver its services or meet its statutory obligations. The College communicates clearly to individuals, at the point of data collection, which processing is consent-based and which proceeds on another lawful basis.

7.2 Special Category Personal Data

The College processes Special Category Personal Data only where, in addition to a lawful basis under Article 6, one of the additional conditions under Article 9 UK GDPR is met. Applicable conditions include:

- explicit consent from the data subject
- processing necessary for employment, social security or social protection law purposes
- processing necessary to protect the vital interests of the data subject

- processing necessary for health or social care purposes
- processing necessary for equality monitoring purposes

Where processing is based on explicit consent, the College ensures that consent is obtained through a clear, affirmative act and is documented.

7.3 Criminal Convictions and Offences Data

The College processes criminal convictions and offences data only where it holds official authority to do so, or where specific legal authorisation applies. This data is treated as distinct from Special Category Data under Article 10 UK GDPR and is subject to additional safeguards. It is held separately from other personal data.

7.4 Consent

Where the College relies on consent as its lawful basis for processing, that consent must be:

- freely given, specific, informed and unambiguous
- obtained at the point of data collection, separately from other terms or conditions
- documented and capable of being evidenced

Individuals may withdraw consent at any time by contacting the DPO at dpo@ukcbc.ac.uk or, where available, through their online record. Withdrawal does not affect the lawfulness of processing carried out before withdrawal. The College does not make consent a condition of providing a service where another lawful basis applies.

7.5 Marketing Communications

The College sends promotional or marketing communications only where the individual has given prior consent to receive them. Consent for marketing may be withdrawn at any time by using the unsubscribe function in any marketing communication or by updating preferences through the relevant online account.

The College does not share contact details with third parties for marketing purposes.

8. Data Subject Rights

The College upholds all data subject rights under UK GDPR. All data subjects may exercise the rights set out below by contacting the DPO at dpo@ukcbc.ac.uk. Full procedures for handling data subject rights requests are set out in DIG 2.7.

8.1 Right of Access

Data subjects have the right to obtain confirmation that the College is processing their personal data and to receive a copy of that data. Current students and staff may view much of their data directly through their online record or staff portal.

8.2 Right to Rectification

Data subjects have the right to have inaccurate personal data corrected and incomplete personal data completed without undue delay.

8.3 Right to Erasure

Data subjects have the right to have their personal data erased in certain circumstances, including where it is no longer necessary for the purpose for which it was collected. The College considers each request carefully against any legal or regulatory obligation to retain the data. Where a request for erasure relates to Special Category Data, particular care is taken to balance the request against overriding legal obligations.

8.4 Right to Restriction of Processing

Data subjects have the right to restrict processing in certain circumstances, including where they contest the accuracy of the data or object to processing pending verification of legitimate grounds.

8.5 Right to Data Portability

Data subjects have the right to receive their personal data in a structured, commonly used and machine-readable format and to transmit it to another controller. Individuals may request their biographical record as a CSV file by contacting the DPO.

8.6 Right to Object

Data subjects have the right to object to the processing of their personal data, including for direct marketing purposes. Where processing is based on legitimate interests, the College ceases processing unless it can demonstrate compelling legitimate grounds that override the data subject's interests.

8.7 Rights Related to Automated Decision-Making

The College does not make solely automated decisions that have legal or similarly significant effects on individuals. Where automated tools are used, for example to monitor student progress and generate alerts for academic staff, those tools inform human decision-making and do not replace it. Staff retain responsibility for any consequent action.

8.8 Responding to Requests

The College responds to valid data subject rights requests within one calendar month of receipt. This period may be extended by a further two months where requests are complex or numerous; the College notifies the data subject of any extension within the first month.

The College may request verification of identity before processing a request. Where a request involves the personal data of third parties, the College balances disclosure obligations against the privacy rights of those individuals. Certain exemptions under the DPA 2018 may apply; the DPO assesses each request individually.

Staff who receive a data subject rights request must refer it to the DPO without delay.

8.9 Right to Complain

Data subjects have the right to lodge a complaint with the ICO at any time if they consider that the processing of their personal data infringes UK GDPR. The ICO can be contacted at https://www.ico.org.uk or by telephone on 0303 123 1113. The College encourages data subjects to contact the DPO in the first instance to allow any concern to be addressed directly.

9. Data Sharing and Third-Party Processing

9.1 General Principle

The College does not provide personal data to third parties for their own independent use, except:

- where required by law, including provision to statutory bodies in territories where the College operates
- where necessary for authorised data processors engaged in the College's operations
- where the data subject has given specific consent

9.2 Statutory and Academic Partners

The College shares data with statutory and academic partners where required for the delivery of its services. This includes:

- partner universities (University of West London, Plymouth Marjon University and Ravensbourne University London) to confirm student progress and award, and to enable HESA reporting
- awarding bodies including Pearson (BTEC/HND), AAT and ACCA, to enable confirmation of qualifications
- regulatory bodies such as the Office for Students and Student Finance England, where disclosure is required by law
- law enforcement agencies, legal advisors and other statutory bodies, where the College is legally obliged to disclose

Disclosure to statutory bodies is made only where it is lawful and necessary for the recipient to perform its statutory functions.

9.3 Data Processing Agreements

Where the College engages third-party data processors, a Data Processing Agreement (DPA) must be in place before any processing begins. The College's standard DPA template must be used wherever possible.

The DPA must require the processor to:

- process personal data only on the College's documented instructions
- ensure all personnel authorised to process the data are subject to appropriate confidentiality obligations
- implement appropriate technical and organisational security measures
- obtain the College's prior written consent before engaging sub-processors, and impose equivalent obligations on them

- assist the College in responding to data subject rights requests
- support the College in meeting its obligations on breach notification, DPIAs and prior consultation with the ICO
- delete or return all personal data on termination of the contract, unless retention is required by law
- make available all information necessary to demonstrate compliance with Article 28 UK GDPR and permit audits or inspections

Where a proposed processing arrangement triggers a DPIA, the DPO must be consulted before the agreement is entered into.

9.4 International Transfers

The College does not transfer personal data to countries outside the UK unless:

- the receiving country ensures an adequate level of protection as recognised by the ICO
- appropriate safeguards are in place, such as an International Data Transfer Agreement (IDTA) or the UK Addendum to EU Standard Contractual Clauses
- one of the specific derogations under UK GDPR applies

Where the College operates outside the UK, including at its Dubai campus, it applies the transfer mechanisms required under applicable local data protection law, including the UAE PDPL where relevant.

The College does not share student contact details with third parties for marketing purposes.

10. Data Security

10.1 Technical and Organisational Measures

The College implements appropriate technical and organisational measures to protect personal data against unauthorised or unlawful processing and against accidental loss, destruction or damage. These measures include:

- pseudonymisation and encryption of personal data where appropriate
- controls to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems

- processes to restore the availability and access of personal data in a timely manner following a physical or technical incident
- regular testing, assessment and evaluation of the effectiveness of security measures

10.2 Access Controls

The College operates strict access controls to ensure that:

- only authorised individuals can access personal data
- access is granted on the basis of legitimate business or academic need
- access is removed promptly when no longer required
- strong password policies are enforced and multi-factor authentication is used where appropriate

Personal data is shared only with staff who require access to perform their roles. Access is restricted by the records a member of staff is authorised to view, the data items within those records, and the actions they are authorised to perform.

All personal data is held on servers located within the United Kingdom and controlled by the College, with the exception of data held on the student portal and financial transaction data, which are held within secure cloud-based systems.

10.3 Student Portal

On the College's student portal, a student's name and profile photograph are visible to other students in their class and to lecturers and module leaders. No other personal information is visible to other students by default.

Students can edit or hide their profile information and control messaging preferences through their portal profile settings. An administrative team oversees the portal and has access to all content solely for the purposes of responding to complaints or reported issues.

10.4 Data Security Breaches

Any actual or suspected personal data breach must be reported to the DPO immediately and without undue delay following discovery. Staff must not attempt to investigate, resolve or conceal a breach before reporting it.

On receiving a breach report, the DPO will:

- assess the likely risk to individuals' rights and freedoms
- determine whether the breach must be reported to the ICO within 72 hours of the College becoming aware of it
- determine whether affected data subjects must be notified without undue delay
- record the breach in the College's Data Breach Log regardless of whether ICO notification is required

All breaches are investigated and reviewed to identify root causes and prevent recurrence. The Data Breach Log is maintained by the DPO and reviewed periodically by the Data Policy Oversight Group.

11. Retention and Secure Disposal

The College retains personal data only for as long as is necessary for the purposes for which it was collected, or as required by legal or regulatory obligation. Full retention schedules are set out in the Records Management and Data Retention Policy (DIG 2.4). The following standard periods apply:

Category	Standard Retention Period
Staff employment records	6 years after end of employment
Prospect / enquiry information	1 year
Unsuccessful applications	18 months
Student information (no award made)	6 years
Student information (award made)	Permanent (award details only)
Third parties (agents, examiners)	1 year after interaction ends

Personal data is retained beyond standard periods only where it has been fully anonymised. All data held in any format is updated and deleted in accordance with the applicable retention schedule. Paper records are archived and destroyed via an approved contractor. Digital records are securely deleted at the end of the applicable retention period.

12. Records and Documentation

The College maintains records of its processing activities in accordance with Article 30 UK GDPR. These records include:

- the purposes of processing
- categories of data subjects and personal data
- categories of recipients to whom personal data is or may be disclosed
- details of transfers to third countries
- retention periods
- technical and organisational security measures

The College documents its compliance through policies, procedures, training records, audit reports and DPIAs. These records are maintained by the DPO and are available for inspection by the ICO on request.

13. Training and Awareness

The College provides appropriate data protection training to all staff and relevant data users, including:

- induction training for new staff covering data protection legislation and this policy
- regular refresher training to maintain awareness
- specialist training for staff with particular data protection responsibilities
- guidance for students where their academic activities involve processing personal data

The Head of People and Culture maintains records of training completion. Training completion rates are monitored by the Data Policy Oversight Group as part of ongoing compliance oversight.

14. What This Means for You

14.1 For Staff

You must handle personal data securely, access it only for legitimate work purposes, and report any concerns or suspected breaches to the DPO without delay. You must complete data protection training as required. Unauthorised disclosure of personal data may result in disciplinary action or, in serious cases, referral to the relevant authorities.

14.2 For Students, Prospects and Applicants

The College collects and uses your personal data to deliver educational services, support your studies and meet its legal obligations. You have the right to access, correct and, in certain circumstances, request deletion of your personal data. You can exercise these rights by contacting the DPO at dpo@ukcbc.ac.uk or by logging in to your student portal.

If you are studying at the College's Dubai campus, your personal data is also protected under the UAE Personal Data Protection Law (Federal Decree-Law No. 45 of 2021) in addition to the College's general data protection commitments.

14.3 For Contractors and Third-Party Processors

You must comply with the data protection requirements set out in your Data Processing Agreement with the College. You must process personal data only on the College's documented instructions, implement appropriate security measures, and notify the College without delay of any actual or suspected breach.

15. Monitoring and Review

15.1 Compliance Monitoring

The DPO and Data Policy Oversight Group monitor compliance with this policy through:

- periodic audits of data processing activities
- review of data security incidents and near misses
- assessment of training completion rates

- review of data subject rights requests and complaints

15.2 Policy Review

This policy is reviewed at least every two years or earlier if required by:

- changes to data protection legislation or ICO guidance
- changes to the College's operational structure or systems
- findings from compliance audits or data security incidents

The Operations Committee is responsible for approving this policy following review.

16. Linked Policies

This policy must be read in conjunction with the following College documents:

- DIG 2.3 Student Privacy Notice
- DIG 2.4 Records Management and Data Retention Policy
- DIG 2.6 Information Security and Acceptable Use Policy
- DIG 2.7 Subject Access Request and Individual Data Rights Policy
- HSE 4.4 Cookie Policy
- SLCC 6.1 Terms and Conditions
- SLCC 6.12 Admissions Policy and Procedure
- Staff Code of Conduct
- Student Code of Conduct

17. External Reference Points

This policy is informed by:

- UK General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018 (DPA 2018)
- Privacy and Electronic Communications Regulations 2003 (PECR)
- Data (Use and Access) Act 2025

- UAE Personal Data Protection Law (Federal Decree-Law No. 45 of 2021)
- Information Commissioner's Office guidance and codes of practice

18. Contact Information

Data Protection Officer: dpo@ukcbc.ac.uk

UK Campus:

United Kingdom College of Business and Computing

Eastgate House, 40 Duke's Place, London, EC3A 7LP

Tel: 020 8518 4994 | info@ukcbc.ac.uk | www.ukcbc.ac.uk

Dubai Campus:

United Kingdom College of Business and Computing Dubai

Dubai International Academic City, Block 10, Second Floor, Dubai, UAE, PO Box 345036

info@ukcbc.ac.ae

19. Version Control Table

Version	Date	Author	Summary of Changes
1.0	Nov 2018	Ben Stedman	Initial Data Protection Policy created
2.0	Sept 2019	Ben Stedman	
3.0			
4.0	Sept 2022	Ben Stedman	Updated to reflect legislative changes
5.0 (DIG 2.1)	Jan 2026	Pauline Williams	Comprehensive revision to align with GA 3.1. Enhanced committee structure, strengthened procedures, corrected approving committee, restructured for compliant numbering.
5.1 (DIG 2.2)	Jan 2026	Pauline Williams	Standalone policy for prospects, applicants and students. Comprehensive revision aligned with GA 3.1.
6.0	May 2026	Pauline Williams	Consolidation of DIG 2.1 (staff) and DIG 2.2 (students) into a single unified policy covering all data subjects. UAE PDPL provisions incorporated. Role-based responsibilities maintained. Policy renumbered DIG 2.1 v6. DIG 2.2 retired.