



UKCBC Privacy Notice

Policy no:	DIG 2.3
Version no. & date:	Version 4.1 – 23 October 2026
Policy Owner	Chief Academic Officer
Last review date:	23 October 2026
Next review date:	October 2028
Responsible Committee:	College Management Team (CMT)
Approved by & date:	College Management Team (CMT) – 23 October 2026
External reference points:	UK General Data Protection Regulation (UK GDPR) Data Protection Act 2018 Data (Use and Access) Act 2025 Privacy and Electronic Communications Regulations (PECR) Office for Students (OfS) Regulatory Framework
Linked policies:	DIG 2.1 Data Protection and Confidentiality Policy, DIG 2.4 Records Management and Data Retention Policy DIG 2.8 Cookie Policy SLCC 6.3 Complaints Policy HSE 4.4 CCTV Policy
Audience:	Prospects, Applicants, Current Students, Former Students

1. Purpose

This privacy notice explains how UK College of Business and Computing (UKCBC or the College) collects, uses, stores and protects your personal information in accordance with UK data protection law. The College is committed to protecting your privacy and handling your personal data responsibly.

1.1 Who This Notice Applies To

This notice applies to:

- Prospects enquiring about courses
- Applicants going through the admissions process
- Current students enrolled on programmes
- Students on a break or deferral from study
- Former students and graduates

1.2 Data Controller

UKCBC is the data controller for the personal data the College processes about you. This means the College decides how and why your data is used and the College is responsible for keeping it safe and handling it lawfully.

1.3 Legal Framework

The College processes your data in accordance with the UK General Data Protection Regulation (UK GDPR), Data Protection Act 2018, Data (Use and Access) Act 2025, and the Privacy and Electronic

Communications Regulations (PECR). Where relevant, the College also complies with equivalent legislation in the United Arab Emirates.

2. What Personal Data the College Collects

The College collects different types of personal data depending on your relationship with UKCBC. The College only collects information that is needed to provide services to you and meet legal obligations.

2.1 Contact and Identity Information

The College collects basic information to identify you and communicate with you:

- Full name and any previous names
- Date of birth
- Contact details (postal address, email address, telephone numbers)
- Emergency contact details (for enrolled students)
- Photographic identification (passport, driving license)

2.2 Course and Academic Information

The College collects information about your studies:

- Courses you enquire about or apply for
- Previous education and qualifications
- Academic references
- Attendance records

- Assessment submissions and results
- Academic progression information
- Details of any breaks in study, deferrals or programme changes

2.3 Equality and Support Information

The College collects information to understand the student community and provide appropriate support. This information is only collected if you choose to provide it and at the appropriate stage of your journey with the College:

- Ethnicity
- Gender identity
- Religious belief
- Disability or health conditions requiring support
- Special educational needs

This information helps the College meet legal obligations to UK Government higher education agencies and ensure the College provides appropriate support throughout your studies.

2.4 Financial Information

Where you make payments or receive refunds:

- Bank account details (for refunds or direct payments)
- Student loan information (where applicable)

The College never stores payment card details. Card payments are processed securely through approved payment providers.

2.5 Communications and Records

The College keeps records of interactions with you:

- Email correspondence
- Messages through the student portal and virtual learning environment
- Records of meetings and telephone conversations
- Documents you submit (applications, appeals, complaints)
- Profile information on learning platforms

2.6 Surveillance and CCTV Data

The College operates closed-circuit television (CCTV) systems at its premises for the purposes of:

- Ensuring the safety and security of students, staff and visitors
- Preventing and detecting crime
- Protecting College property and assets

CCTV cameras are positioned at entrances, corridors, classrooms and other communal areas inside the College campuses. Signage is displayed prominently at entry points and within areas monitored by CCTV to ensure individuals are informed that surveillance is in operation.

CCTV footage may capture your image and movements while you are on college premises. This data is retained for a minimum 30-day period necessary for security and safety purposes, in line with ICO guidance on surveillance.

3. How the College Collects Your Data

The College collects personal data through various channels.

3.1 Directly from You

Most of your data comes directly from you when you:

- Complete enquiry forms on the College website or social media
- Submit an application through the online system
- Enrol as a student and complete registration forms
- Submit coursework and assessments
- Contact the College by email, phone or through student systems
- Use the virtual learning environment (VLE) or student portal
- Update your details on Student360

3.2 From Third Parties

The College may receive data about you from:

- Educational agents acting on your behalf (with your consent)
- Referees providing academic or professional references
- Awarding bodies and partner universities
- Student Finance England or equivalent bodies

All data the College receives from third parties is processed lawfully and with appropriate safeguards.

3.3 Through Surveillance Systems

The College collects CCTV footage automatically through surveillance systems positioned at college premises, as described in Section 2.6.

4. Why the College Uses Your Data (Legal Basis)

The College only uses your personal data when there is a legal basis to do so under data protection law. The legal bases the College relies on are:

4.1 Contract

When you apply to study with the College or enrol as a student, you enter into a contract with UKCBC. The College needs to process your data to:

- Process your application
- Enrol you on your chosen programme
- Deliver teaching and learning services
- Assess your work and award qualifications
- Manage your student account and finances
- Respond to queries and complaints

The College also relies on contract to share your data with awarding bodies and partner universities (Section 5.1) and professional awarding organisations (Section 5.2), as this sharing is necessary to deliver the qualification you have enrolled for.

4.2 Legal Obligation

The College must process certain data to comply with UK law and regulatory requirements, including:

- Reporting to the Office for Students (OfS)
- Providing data to the Higher Education Statistics Agency (HESA)
- Confirming awards to professional bodies
- Responding to lawful requests from regulatory or law enforcement bodies
- Compliance with counter-terrorism obligations (Prevent duty)

The College relies on legal obligation when sharing data with UK Government and regulatory bodies as described in Section 5.3, and when responding to lawful requests as described in Section 5.5.

4.2.1 Prevent Duty and Safeguarding

Under the Counterterrorism and Security Act 2015, the College has a statutory duty to prevent people from being drawn into terrorism. Where there are legitimate safeguarding concerns that a student may be vulnerable to radicalisation or at risk of serious harm, the College's Designated Safeguarding Lead may share relevant student information on a need-to-know basis with:

- Local authority Prevent Team or Channel Panel
- Police authorities (including Counter-Terrorism Policing)
- Local safeguarding partners (health services, social services)
- Home Office or other government departments, where mandated by law

Information shared for this purpose may include a student's name, date of birth, student ID and contact details, course details and attendance records, and information relating to safeguarding concerns, risk

assessments or behavioural incidents. Particularly sensitive information, such as data about religion or health, is shared only where this is essential and justified.

4.3 Consent

Where the College has asked for your consent, the College uses your data for:

- Sending you marketing communications about courses and events (as described in Section 10)
- Using your images or testimonials in promotional materials
- Sharing information beyond what is required by contract or law

You can withdraw your consent at any time by contacting the College. For marketing communications, you can opt out using the methods described in Section 10.

4.4 Legitimate Interests

The College may process your data where there is a legitimate interest that does not override your rights. This includes:

- Improving courses and services through internal analysis
- Monitoring attendance to identify students who may need support
- Preventing and detecting fraud
- Protecting the security of IT systems
- Managing facilities and ensuring campus safety through CCTV surveillance (as described in Section 2.6)
- Analysing aggregated, anonymised website usage data, collected via cookies you have consented to, to improve the website (as described in Section 11)

The College always balances its interests against your rights and will not use your data in ways you would not reasonably expect. Cookies themselves are not placed on the basis of legitimate interests. Except where strictly necessary for the website to function, cookies, including those used for analytics, are only set with your consent, as explained in Section 11 and the DIG 2.8 Cookie Policy.

5. Who the College Shares Your Data With

The College only shares your personal data when necessary and with appropriate safeguards. The College never sells your data to third parties.

5.1 Awarding Bodies and Partner Universities

When you study for a qualification awarded by a partner institution, the College must share your data with them:

- University of West London (UWL): For undergraduate and postgraduate programmes validated by UWL, the College shares identity, contact, course enrolment, attendance, assessment and award information.
- Plymouth Marjon University (PMU): For programmes validated by PMU, the College shares equivalent information to support your progression and award.
- Ravensbourne University London (RUL): For programmes validated by RUL, the College shares equivalent information to support your progression and award.

These partner institutions process your data as independent data controllers and are subject to their own privacy notices. They also provide data to the Higher Education Statistics Agency (HESA) as required by UK Government.

5.2 Professional and Vocational Awarding Organisations

For vocational qualifications, the College shares data with:

- Pearson: For BTEC and Higher National Diploma (HND) qualifications, the College shares identity, biographical and assessment data
- Association of Accounting Technicians (AAT): For AAT qualifications, the College shares equivalent data
- Association of Chartered Certified Accountants (ACCA): For ACCA qualifications, the College shares equivalent data

5.3 UK Government and Regulatory Bodies

The College reports data to UK Government agencies as required by law:

- Office for Students (OfS): Regulatory and compliance reporting
- Higher Education Statistics Agency (HESA): Statistical returns on students and outcomes
- Student Finance England: Confirmation of attendance and completion for loan recipients
- Home Office: Counterterrorism and safeguarding reporting where required

5.4 Other Third-Party Processors

The College uses carefully selected service providers to support operations:

- IT service providers hosting student management systems and VLE
- Cloud storage providers (with servers located in the UK)
- Communication platforms for emails and messaging
- Payment processing services (who do not store full card details)
- Document destruction services for secure disposal of records

All third-party processors are required to protect your data and only use it on the College's instructions.

5.5 Legal Requirements

The College may disclose your data where required by law to:

- Police or law enforcement agencies
- Courts and legal advisors
- Health and safety authorities
- Other regulatory or government bodies

The College only discloses data when legally required and limits disclosure to what is necessary.

6. Transferring Data Outside the UK

Your personal data is stored on College systems hosted in the UK. Some of this data is transferred outside the UK, or accessed from outside the UK by people who support the College's work. Under UK data protection law, giving someone outside the UK access to your data counts as a transfer, even when the data stays on UK servers. The College only makes these transfers where your data remains protected to the standard that UK law requires.

6.1 Cloud Services in the European Economic Area

Some College systems use cloud providers with servers in the European Economic Area (EEA). UK law recognises the EEA as providing an adequate level of protection for personal data, so these transfers do not need additional safeguards.

6.2 Support Services Provided from India

The College uses an external provider based in India to deliver:

- IT helpdesk support for students, applicants and members of the public
- Software development and testing for College systems
- Admissions and marketing support, including creating and maintaining applicant records

To deliver these services, the provider's staff access College systems remotely. Depending on the service, this may include your contact and identity information, your application and qualification details and the equality information described in Section 2.3.

The provider acts only on the College's documented instructions and does not hold your data on its own systems. Under its contract with the College:

- Your data must stay on College systems hosted in the UK
- The provider's staff must not download, copy or store your data anywhere else
- Each member of the provider's staff must use an individual account that the College creates, audits and can withdraw
- The provider's staff must complete the College's data protection training before they receive access
- The provider must not share your data with any other organisation or use another organisation to process it
- Software development and testing must use anonymised data, with any access to live records strictly controlled

UK law does not recognise India as providing an adequate level of protection. The College therefore protects these transfers through the International Data Transfer Agreement (IDTA) issued by the Information Commissioner's Office (ICO).

6.3 Dubai Campus

The College operates a campus in Dubai, United Arab Emirates. Some staff based at the Dubai campus have controlled access to College systems hosted in the UK, where this is necessary to provide educational and administrative services.

6.4 Other Transfers

If the College needs to transfer your data to any other organisation outside the UK, such as a partner institution, it only does so where UK law recognises the destination as providing adequate protection or where appropriate safeguards are in place. These safeguards include the IDTA and the UK Addendum to the EU Standard Contractual Clauses.

You can ask for more information about any of the safeguards described in this section, including a copy of the relevant transfer agreement, by emailing dpo@ukcbc.ac.uk.

7. How Long the College Keeps Your Data

The College retains your personal data only for as long as necessary to fulfil obligations to you and meet legal and regulatory requirements. Retention periods vary depending on the nature of the data and your relationship with UKCBC.

7.1 Enquiry Information

Retained for: 1 year from last contact

Purpose: To respond to your enquiry and provide relevant course information

7.2 Unsuccessful Applications

Retained for: Up to 18 months from application date

Purpose: To process your application and respond to any appeals or queries

7.3 Student Records (No Award Made)

Retained for: Up to 6 years from last enrolment date

Purpose: To comply with legal obligations, respond to queries and maintain accurate records

7.4 Student Records (Award Made)

Where you have been awarded a qualification, the College retains the following information permanently:

- Full legal name (as appears on the award certificate)
- Date of birth
- Student identification number
- Programme title and level (e.g., BA (Hons) Business Management)
- Award classification (e.g., First Class Honours, Merit, Pass)
- Date of award
- Awarding body (e.g., University of West London)

Purpose of permanent retention: The College has a continuing obligation to verify your qualifications throughout your lifetime. Employers, professional bodies, further education providers and other organisations may contact the College to confirm the authenticity of your qualification. The College must be able to provide accurate verification and issue replacement transcripts or certificates when requested by you or by third parties with your consent. Permanent retention of core award information enables the College to meet these obligations and protect the integrity of qualifications.

All other student data (including contact details, attendance records, assessment submissions, and correspondence) is retained for up to 6 years after completion in accordance with the College's DIG 2.4 Records Management and Data Retention Policy.

7.5 Third-Party Relationships

Retained for: Up to 1 year after last interaction

Purpose: To manage relationships with agents, examiners and service providers.

After these retention periods, data is either securely destroyed or anonymised for statistical purposes. Paper records are destroyed through approved secure destruction contractors.

7.6 CCTV Footage

Retained for: The minimum 30-day period necessary for security and safety purposes, in line with ICO guidance on surveillance.

Purpose: Security, safety and crime prevention. Footage may be retained longer where it records an incident requiring investigation or has been requested by law enforcement.

8. Your Rights

You have important rights over your personal data under UK data protection law.

8.1 Right of Access

You can request a copy of the personal data the College holds about you. Much of this information is available through your Student360 account. For a full copy of your personal data, email dpo@ukcbc.ac.uk

Please note that where the College retains award information permanently (as described in Section 7.4), this information will be included in any subject access request response as it forms part of your personal data held by the College.

If you wish to receive certain data in a portable, machine-readable format to transfer to another organisation, please see Section 8.6 regarding your right to data portability.

8.2 Right to Rectification

If information the College holds about you is inaccurate or incomplete, you can ask the College to correct it. Contact your Admissions Team (if applying) or the Student Support and Experience Team (if enrolled) to update your records.

8.3 Right to Erasure

In limited circumstances, you can request deletion of your data. This right does not apply where the College needs to retain data to:

- Fulfil the contract with you (while you are studying)
- Comply with legal obligations (for example, awarding body requirements, regulatory reporting)
- Establish, exercise or defend legal claims (for example, during appeals or complaints)

8.4 Right to Restrict Processing

You can ask the College to restrict how it uses your data in certain situations, such as when you contest the accuracy of the data or object to processing.

8.5 Right to Object

You have the right to object to processing based on legitimate interests, including:

- Marketing communications: You can opt out at any time via the unsubscribe link in emails or through your Student360 account
- Direct marketing: You can object at any time without providing a reason

8.6 Right to Data Portability

You can request certain personal data in a structured, commonly used, machine-readable format (such as comma separated values (CSV)) to transfer to another organisation. This right applies only to personal data that:

- You have provided to the College, and
- Is processed on the basis of contract or consent, and
- Is processed by automated means

This typically includes data such as:

- Your contact and biographical information
- Course enrolment and progression data
- Assessment results and award information
- Information you have submitted through online forms or student systems

Data processed under legal obligation or legitimate interests (such as regulatory reporting data or CCTV footage) is not subject to the portability right, though it remains accessible through a subject access request under Section 8.1.

8.7 Rights Related to Automated Decision-Making

UKCBC does not use fully automated decision-making or profiling in admissions, assessment or student support decisions. Where the College uses automated systems to identify students who may need additional support (such as attendance alerts), these always involve human review and intervention.

8.8 How to Exercise Your Rights

To exercise any of these rights, contact:

Email: dpo@ukcbc.ac.uk

Phone: 020 8518 4994

Post: Data Protection Officer, UKCBC, Eastgate House, 40 Dukes Place, London, EC3A 7LP

The College will respond to requests within one month. In complex cases, this may be extended by up to two months, and the College will inform you if this is necessary.

9. Keeping Your Data Secure

The College takes the security of your personal data seriously and implements appropriate technical and organisational measures to protect it.

9.1 Technical Security

- All student systems require secure authentication (username and password)
- Regular security updates and patches are applied to systems
- Access to systems is monitored and logged
- Regular backups are maintained to prevent data loss

9.2 Organisational Security

- Staff only have access to data necessary for their role
- All staff complete mandatory data protection training during induction
- Strict access controls limit who can view, edit or delete data
- The College uses role-based permissions across all systems
- Third-party processors are subject to contractual data protection obligations

9.3 Learning Platform Security

On learning platforms (VLE and student portal):

- Your profile information is visible only to students in your class and relevant academic staff
- You control who can send you messages

- Administrative staff have access only to respond to reported issues or complaints

The College does not operate automated or continuous monitoring of communications on learning platforms. Where a concern is raised by a student or staff member, or referred by teaching or non-teaching staff, this is reviewed and handled by the Safeguarding Team in line with the College's Safeguarding policies and procedures.

10. Marketing Communications

The College may contact you about:

- Courses, programmes and events that may interest you
- Open days and application deadlines
- Alumni news and networking opportunities (for graduates)

You control your marketing preferences:

- Opt out at any time using the unsubscribe link in emails
- Update preferences through your Student360 account
- Contact the College at info@ukcbc.ac.uk to change your preferences

The College never shares your contact details with third parties for marketing purposes.

11. Cookies and Website Analytics

The College website uses cookies to support essential website functions and where you have given consent, to analyse website usage and improve services. Strictly necessary cookies do not require consent. Other cookies, including analytics cookies, are only used with your consent and can be managed or withdrawn at any time.

For detailed information about the use of cookies, please see the College's DIG 2.8 Cookie Policy.

12. Complaints and Concerns

If you have concerns about how the College handles your personal data:

1. Contact the Data Protection Officer:

Email: dpo@ukcbc.ac.uk

Phone: 020 8518 4994

Post: Data Protection Officer, UKCBC, Eastgate House, 40 Dukes Place, London, EC3A 7LP

2. The College aims to resolve concerns about how it handles your personal data as quickly as possible. If you wish to raise a formal complaint about any aspect of College services (including data protection matters), please refer to the College's SLCC 6.3 Complaints Policy, which sets out the formal complaints procedure.

3. If you are not satisfied with the College's response, you have the right to complain to the Information Commissioner's Office (ICO):

Website: www.ico.org.uk

Phone: 0303 123 1113

Post: Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF

13. Changes to This Privacy Notice

The College may update this privacy notice from time to time to reflect changes in law, regulation or practices. Significant changes will be:

- Notified to current students via email and through Student360
- Posted prominently on the College website (www.ukcbc.ac.uk)

The current version and date are always shown at the top of this notice.

14. Contact Information

UK College of Business and Computing (UKCBC)

Eastgate House, 40 Dukes Place, London, EC3A 7LP

Phone: 020 8518 0978

Dubai Campus:

UK College of Business and Computing Dubai

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

Dubai, United Arab Emirates

Phone: +971554176201

Email: info@ukcbc.ac.ae

Data Protection Officer:

Email: dpo@ukcbc.ac.uk

Phone: 020 8518 4994

Website: www.ukcbc.ac.uk

Version History

Version	Date	Author	Summary of changes	Approved by
1.0				
2.0				
3.0	May 2019	Ben Stedman		
4.0	June 2026	Pauline Williams	Comprehensive revision to align with GA 3.1 Policy Preparation and Structure Guidance, enhanced committee structure, strengthened procedures Key changes include reclassification as a Student Privacy Notice with clear versioning; plain-language rewrite and compliant structure; explicit identification of UKCBC as data controller; detailed lawful bases, retention periods and international transfer safeguards; expanded rights, complaints and security sections; clearer data-sharing disclosures; updated UK GDPR terminology and current institutional references; removal of redundant, vague or misleading content.	
4.1	23 October 2026	Chief Academic Officer	Role titles updated following organisational restructure; cross references updated for approval; approved by College Management Team (CMT) on 23 October 2026 Stray character removed, footers aligned to Version 4.1 and abbreviations spelt out, in line with GA 3.1 (25 October 2026). Version History table aligned with the suite (26 October 2026).	College Management Team (CMT)