



Subject Access Request and Individual Data Rights Policy

Policy number:	DIG 2.7
Version number and date:	Version 5.0 – June 2026
Author:	Pauline Williams
Policy Owner:	Director of Governance Quality and Student Success
Last review date:	March 2026
Next review due:	June 2028
Responsible Committee:	Operations Committee
Approved by and date:	CMT – 10 June 2026
External reference points:	UK General Data Protection Regulation (UK GDPR) Data Protection Act 2018 Freedom of Information Act 2000 ICO Guidance on Subject Access Requests UAE Federal Decree-Law No. 45 of 2021 on the Protection of Personal Data (UAE PDPL)
Linked policies:	DIG 2.1 Data Protection and Confidentiality Policy DIG 2.4 Records Management and Data Retention Policy
Audience:	All staff

Table of Contents

1. Purpose	1
2. Scope	1
3. Definitions	2
4. Roles and Responsibilities	3
4.1 Overview	3
4.2 Data Protection Officer	3
4.3 All Staff	4
4.4 Departmental Data Owners	4
5. Subject Access Requests	5
5.1 The Right of Access	5
5.2 How a SAR Can Be Submitted	5
5.3 Required Content of a SAR Response	6
5.4 Timescales	6
5.5 Fees and Manifestly Unfounded or Excessive Requests	7
5.6 Process for Handling Subject Access Requests	7
6. Exemptions	7
7. Right to Erasure	9
7.1 When the Right to Erasure Applies	9
7.2 Data UKCBC Must Retain	10
7.3 Process for Handling Erasure Requests	10
8. Right to Rectification	10
8.1 Process for Handling Rectification Requests	11
9. Identity Verification	11
10. Freedom of Information Act 2000	11
11. Security, Retention, and Disposal of SAR Materials	12
11.1 Secure Storage	12
11.2 Retention Period	13
11.3 Disposal	13
12. Record Keeping	13
12.1 What Must Be Recorded	13
12.2 Retention of the Register	14
12.3 Responsibility	14
13. Response Templates	14
14. Monitoring and Review	16
15. Linked Policies	16
16. External References	16

Appendix 1 — ICO Assurance Checklist	18
Version History	19
Annex A	20
SAR and Individual Data Rights Procedure	20
A3. Subject Access Requests — Step-by-Step Process	20
A3.1 Overview	20
A3.2 Process	20
A4. Erasure Requests — Step-by-Step Process	23
A4.1 Overview	23
A4.2 Process	23
A5. Rectification Requests — Step-by-Step Process	25
A5.1 Overview	25
A5.2 Process	25
A6. Identity Verification — Accepted Documents	26
A7. Exemptions — Quick Reference	29
A8. Response Templates	31
A8.1 Subject Access Request Templates	31
A8.1.1 Full disclosure	31
A8.1.2 Partial disclosure — information withheld under an exemption	32
A8.1.3 No disclosure — all information withheld	32
A8.1.4 Partial disclosure — confidential references	33
A8.2 Erasure Request Templates	34
A8.2.1 Initial acknowledgement	34
A8.2.2 Completion confirmation	34
A8.3 Rectification Request Templates	35
A8.3.1 Completion confirmation	35
A9. SITS Removal Checklist for Students	36
A10. Record Keeping	37
A11. Monitoring and Review	37
A12. Linked Documents	37
Annex A — Version History	38

1. Purpose

This policy sets out how UK College of Business and Computing (UKCBC or the College) manages requests by individuals to exercise their data rights under the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 (DPA 2018). These rights include the right of access (subject access requests), the right to erasure, and the right to rectification.

UKCBC takes its obligations under data protection legislation seriously. Any failure to comply with this policy may be regarded as a disciplinary matter and may constitute a breach of the applicable legislation.

This policy must be read alongside DIG 2.1 Data Protection and Confidentiality Policy and DIG 2.4 Records Management and Data Retention Policy.

2. Scope

This policy applies to all staff employed by, or working on behalf of, UKCBC, including contractors, agency workers, and volunteers, across all UKCBC locations.

It applies to requests made by any individual whose personal data UKCBC holds, including:

- current and former students, applicants, and prospects
- current and former staff
- alumni
- contractors and suppliers
- agents and sponsors
- visitors and members of the public

This policy covers personal data held in any format, including digital records, paper files, emails, CCTV footage, and audio recordings.

It applies to UKCBC's UK campuses and its Dubai campus. Where the Dubai campus operates in accordance with applicable UAE data protection legislation, including the UAE Federal Decree-Law No. 45 of 2021 on the Protection of Personal Data (UAE PDPL), this policy is applied in conjunction with those requirements. Any conflicts between UK GDPR requirements and UAE PDPL requirements must be referred to the DPO for guidance.

3. Definitions

For the purposes of this policy, the following terms have the meanings set out below.

Personal data: Any information relating to an identified or identifiable living individual. This includes names, identification numbers, location data, online identifiers, and any factors specific to the individual's physical, physiological, genetic, mental, economic, cultural, or social identity.

Special category data: Personal data that is particularly sensitive under Article 9 of the UK GDPR, including data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data used for identification purposes, health data, and data concerning sex life or sexual orientation.

Data subject: The identified or identifiable natural person to whom the personal data relates.

Data controller: The organisation that determines the purposes and means of processing personal data. UKCBC is the data controller for personal data it holds about its students, staff, and other individuals.

Data processor: An organisation or individual that processes personal data on behalf of UKCBC as data controller, in accordance with a written contract.

Subject Access Request (SAR): A request made by or on behalf of a data subject exercising their right of access to their personal data under Article 15 of the UK GDPR.

Right to erasure: The right under Article 17 of the UK GDPR for a data subject to request that UKCBC erases their personal data in specified circumstances. This right is also referred to as the 'right to be forgotten'.

Right to rectification: The right under Article 16 of the UK GDPR for a data subject to require UKCBC to correct inaccurate personal data held about them, or to complete incomplete data.

Exemption: A lawful basis under the UK GDPR, the DPA 2018, or other applicable legislation that permits UKCBC to withhold, redact, or decline to disclose personal data that would otherwise be disclosable in response to a data subject rights request.

Data Protection Officer (DPO): The designated individual responsible for overseeing UKCBC's compliance with data protection legislation and for advising on data subject rights requests. All requests under this policy must be forwarded to the DPO at dpo@ukcbc.ac.uk.

4. Roles and Responsibilities

4.1 Overview

UKCBC must respond to all individual data rights requests, including Subject Access Requests (SARs), requests for erasure, and requests for rectification, in a timely, consistent, and legally compliant manner. Responsibilities are assigned by role rather than by named individual to ensure continuity when staff change and to avoid delays arising from individual availability. All staff must receive appropriate and regular training so they can recognise individual data rights requests, understand their obligation to forward them immediately to the DPO, and support the process in line with statutory requirements and ICO expectations.

4.2 Data Protection Officer

The DPO holds primary responsibility for the management of all individual data rights requests. The DPO must:

- receive and log all individual data rights requests on the SAR/IDR register
- coordinate the response across relevant departments
- advise staff on exemptions, redaction, and legal requirements
- ensure responses are issued within statutory deadlines
- maintain the SAR/IDR register in accordance with section 12 of this policy

4.3 All Staff

Any member of staff who receives a request, whether written or verbal, and regardless of how it is phrased, must:

- recognise that any written or verbal request for personal data, correction, or deletion is likely to be a valid data rights request, even if the individual does not use specific legal language
- forward the request to the DPO immediately at dpo@ukcbc.ac.uk
- avoid making commitments, providing data, or declining the request directly
- treat the existence of the request as confidential and not discuss it with other staff

Line managers must ensure that the staff they manage are aware of and follow these requirements.

4.4 Departmental Data Owners

Depending on the nature of the request, the DPO will instruct the relevant departmental data owners to locate and supply data. The departments likely to hold relevant personal data include:

People and Culture:	Staff records, payroll, contracts, and performance information
Administration:	Student records, admissions, attendance, and assessment data
Procurement:	Supplier and sponsor information
IT:	System logs, email retrieval, and archived data
Finance:	Payment records, invoices, and Student Finance England information

When instructed by the DPO, departmental data owners must:

- conduct a thorough search of all relevant systems and formats within their area
- provide all responsive data to the DPO promptly and within the timeframe specified
- flag any concerns about third-party personal data, potential exemptions, or data that may be subject to a retention obligation

5. Subject Access Requests

5.1 The Right of Access

Under Article 15 of the UK GDPR, data subjects have the right to obtain confirmation of whether UKCBC processes personal data about them, and if so, to receive a copy of that data together with specified supplementary information.

A subject access request can be made by any individual, including students, applicants, staff, governors, parents or guardians, and members of the public. Requests may also be made by a person acting on behalf of a data subject, such as a legal representative.

5.2 How a SAR Can Be Submitted

A SAR may be submitted verbally or in writing, by any means, including:

- email (to dpo@ukcbc.ac.uk or to any UKCBC email address)
- letter
- in person

UKCBC may invite data subjects to use a dedicated mechanism or form, but must not require them to do so. UKCBC must respond to any valid request regardless of how it is submitted.

Where a SAR is submitted electronically, UKCBC should provide the response in electronic format wherever practicable.

5.3 Required Content of a SAR Response

Where UKCBC holds personal data about the data subject, every SAR response must include the following information:

- the purposes of the processing
- the categories of personal data concerned
- the recipients or categories of recipients to whom personal data has been or will be disclosed, including recipients in third countries or international organisations and the safeguards in place for any such transfers (for example, International Data Transfer Agreements (IDTAs) or UK Addendums to EU Standard Contractual Clauses)
- where possible, the envisaged retention period, or, if not possible, the criteria used to determine that period
- the existence of the right to request rectification, erasure, or restriction of processing, and the right to object to processing
- the right to lodge a complaint with the Information Commissioner's Office (ICO)
- where personal data has not been collected directly from the data subject, the source of that data
- the existence of any automated decision-making, including profiling, together with meaningful information about the logic involved, the significance, and the envisaged consequences for the data subject

5.4 Timescales

UKCBC must respond to a SAR within one calendar month of receipt. The calendar month runs from the date of receipt, not from the date on which the request is validated. The response deadline does not pause during College closure periods. The DPO must ensure that contingency arrangements are in place to meet statutory deadlines during planned College closures.

Where a request is complex or involves a large volume of data, UKCBC may extend the response period by a further two months. Where an extension is necessary, UKCBC must notify the data subject within the first calendar month, explaining the reason for the delay.

Where UKCBC determines that it will not take action on a request, it must inform the data subject of this decision, with reasons, within one calendar month of receipt.

5.5 Fees and Manifestly Unfounded or Excessive Requests

UKCBC must respond to SARs free of charge. However, UKCBC may charge a reasonable fee, or may refuse to act on a request, where the request is manifestly unfounded or excessive, particularly where it is repetitive. UKCBC must consult current ICO guidance before applying this exemption, as it is a high threshold to meet.

UKCBC may charge a reasonable fee for providing further copies of the same information following a previous request.

5.6 Process for Handling Subject Access Requests

The DPO must handle all SARs in accordance with the step-by-step process set out in section A3 of Annex A to this policy. Annex A sets out the required steps from receipt through to response, including logging, identity verification, data searches, exemption review, and escalation.

6. Exemptions

Certain personal data may be exempt from disclosure in response to a SAR or other data rights request under the UK GDPR, the DPA 2018, or other applicable legislation. The DPO is responsible for assessing whether an exemption applies in each case.

Common exemptions that may apply in the context of UKCBC include:

Third-party personal data: Where a disclosure would reveal personal data about another individual who has not consented to that disclosure, and it would not be reasonable to disclose without consent, UKCBC must redact that third-party data before responding.

Legal professional privilege: Data that is subject to legal professional privilege, including communications with legal advisers, need not be disclosed.

Management forecasting and planning: Data processed for the purpose of management forecasting or planning in relation to UKCBC's business or activities may be exempt where disclosure would be likely to prejudice the conduct of that business or activity. UKCBC must be able to demonstrate that the personal data is relevant to and being used for that purpose, and that the prejudice to UKCBC from disclosure is greater than the harm to the individual from being denied access. The DPO must document the basis for applying this exemption in each case.

Negotiations: Data consisting of a record of UKCBC's intentions in relation to negotiations with the data subject may be exempt where disclosure would be likely to prejudice those negotiations. This exemption applies only whilst negotiations are ongoing. Once negotiations have concluded, UKCBC cannot rely on this exemption in response to a subsequent request, and the DPO must reassess whether the data falls within any other applicable exemption before withholding it.

Crime and taxation: Data may be exempt from disclosure where doing so would be likely to prejudice the prevention or detection of crime, the apprehension or prosecution of offenders, or the assessment or collection of a tax or duty.

Confidential references: References given in confidence by UKCBC for the purposes of education, training, or employment are exempt from disclosure. References received by UKCBC are also exempt where the referee has not given consent to disclosure.

Safeguarding and Prevent: Where disclosure of personal data would be likely to prejudice vulnerable individual protection or safeguarding activities, or where concerns arise under the Prevent duty, UKCBC must seek DPO and, where appropriate, Designated Safeguarding Lead (DSL) advice before responding.

Exam scripts and examination processes: A student's own examination scripts are exempt from the right of access. Examiner comments are also exempt to the extent that they form part of the examination process. Marks awarded are not exempt.

Where UKCBC withholds or redacts data on the basis of an exemption, it must document the exemption applied and communicate to the data subject that information has been withheld, together with the reason, unless doing so would itself undermine the purpose of the exemption.

UKCBC will seek advice from the ICO where there is uncertainty as to which exemptions apply. A quick-reference summary of exemptions for operational use is provided in section A7 of Annex A.

7. Right to Erasure

7.1 When the Right to Erasure Applies

Under Article 17 of the UK GDPR, individuals have the right to request that UKCBC erases their personal data. The right applies where:

- the personal data is no longer necessary for the purpose for which it was originally collected or processed
- the individual withdraws consent and there is no other lawful basis for processing
- the individual objects to processing based on legitimate interests and there is no overriding legitimate interest to continue
- the individual objects to processing for direct marketing purposes
- the personal data has been processed unlawfully
- erasure is required to comply with a legal obligation

- the personal data was processed to offer information society services to a vulnerable individual

The right to erasure is not absolute. It does not apply where UKCBC is required to retain the data by law, or where processing is necessary for the establishment, exercise, or defence of legal claims. UKCBC must respond to erasure requests within one calendar month of receipt. Where a request is complex, the response period may be extended by a further two months, with notification to the data subject within the first calendar month.

UKCBC will give particular weight to erasure requests where the personal data was collected from a vulnerable individual, including where the individual making the request may no longer be vulnerable.

7.2 Data UKCBC Must Retain

UKCBC must retain certain personal data regardless of an erasure request. This includes data relating to:

- qualifications obtained and records of study
- financial transactions, including Student Finance England (SFE) records
- regulatory reporting obligations to government bodies or funding bodies
- ongoing or anticipated legal proceedings

Where data cannot be erased, UKCBC must inform the data subject of this and explain why.

7.3 Process for Handling Erasure Requests

The DPO must handle all erasure requests in accordance with the step-by-step process set out in section A4 of Annex A to this policy. Annex A sets out the required steps from receipt through to completion confirmation, including the obligation to identify data that must be retained and to document all retention decisions.

8. Right to Rectification

Under Article 16 of the UK GDPR, individuals have the right to require UKCBC to correct inaccurate personal data held about them, and to complete incomplete personal data.

This process must not be used for academic appeals. It does apply where the outcome of an academic appeal has not been reflected in a student's record.

UKCBC will verify the accuracy of the proposed correction and may request supporting evidence before making changes to records.

UKCBC will respond to rectification requests within one calendar month of receipt. Where necessary, the response deadline may be extended by a further two months for complex requests, with notification to the data subject within the first month.

8.1 Process for Handling Rectification Requests

The DPO must handle all rectification requests in accordance with the step-by-step process set out in section A5 of Annex A to this policy. Annex A sets out the required steps from receipt through to completion confirmation, including identity verification, evidence gathering, and instructions to data store owners.

9. Identity Verification

Before releasing, erasing, or correcting any personal data, UKCBC must verify the identity of the data subject making the request. Where a request is made by a third party on behalf of a data subject, UKCBC must also verify the identity of the third party and their authority to act.

The DPO maintains a current list of accepted identification documents as part of Annex A to this policy (section A6). Where a data subject cannot provide acceptable identification, the DPO must advise on the appropriate course of action before any data is released, erased, or corrected.

10. Freedom of Information Act 2000

Some requests may be, or may include requests for information under the Freedom of Information Act 2000 (FOIA). In some cases, individuals may mistakenly refer to the FOIA when they are making a SAR, or vice versa.

UKCBC must correctly identify whether a request is made under the UK GDPR (personal data about the requester) or the FOIA (general information held by UKCBC). Where a request covers both, each element must be dealt with under the applicable regime.

FOIA requests must be dealt with promptly and in any event within twenty working days of receipt. All FOIA requests must be forwarded to the DPO at dpo@ukcbc.ac.uk in the first instance, who will coordinate the response or direct the request to the appropriate designated contact.

Unlike the UK GDPR one-calendar-month deadline, the FOIA 20-working-day deadline counts only working days and therefore excludes weekends and public holidays. The deadline can also be paused whilst UKCBC seeks clarification from the requester about the scope of the request.

11. Security, Retention, and Disposal of SAR Materials

All materials relating to individual data rights requests must be handled securely throughout the request lifecycle. This includes the original request, correspondence, data compiled in response, records of exemptions applied, and confirmation of actions taken.

11.1 Secure Storage

SAR files must be stored securely in a folder or directory designated by the DPO for that purpose, with access restricted to the DPO and any member of staff specifically authorised to assist with the request. SAR files must not be shared more widely than is necessary to fulfil the request.

Where SAR materials are held electronically, access controls must be applied to restrict access to authorised individuals. Where materials are held in paper form, they must be stored in locked cabinets.

11.2 Retention Period

UKCBC retains SAR-related records, including logs, correspondence, and response documentation, for two to three years from the date on which the SAR is closed. This period reflects the UK GDPR storage limitation principle: it is sufficient to demonstrate compliance and to respond to any ICO investigation or legal dispute, which typically arise within 12 to 24 months of the original response, whilst ensuring that records are not kept for longer than necessary. This approach is consistent with UKCBC's wider practice of applying proportionate, purpose-based retention periods across its data holdings. Where a longer period is required by ongoing legal proceedings or a specific regulatory obligation, the DPO must document this decision and review it at regular intervals. The applicable retention schedule is set out in the DIG 2.4 Records Management and Data Retention Policy.

11.3 Disposal

On expiry of the retention period, SAR materials must be disposed of securely:

- electronic files must be permanently deleted and not held in recoverable formats
- paper documents must be shredded or disposed of using a secure waste disposal service

Disposal must be recorded in the IDR register.

12. Record Keeping

The DPO must maintain a formal Individual Data Request (IDR) register. This register supports UKCBC's accountability obligations under Article 5(2) of the UK GDPR and enables compliance monitoring and audit.

12.1 What Must Be Recorded

For every individual data rights request received, the following information must be entered in the IDR register:

- date of receipt of the request

- name of the data subject
- name and address of the requester (if different from the data subject)
- type of request (SAR, erasure, rectification, other)
- type and scope of data involved
- date on which identity was verified
- planned response date
- date of response
- outcome (data disclosed, partially disclosed, withheld, erased, corrected, request declined)
- any exemptions applied, with reasons
- date of any extension notification
- whether a complaint was received and its outcome

12.2 Retention of the Register

The IDR register must be retained for a minimum of three years from the date of the last entry. This retention period applies to the register itself and is separate from, and independent of, the two-to-three-year retention period for individual SAR files set out in section 11.2. The register must be made available to the ICO on request.

12.3 Responsibility

The DPO is responsible for maintaining the IDR register and ensuring that it is accurate, complete, and up to date. The DPO must report on request volumes and outcomes to the Operations Committee as part of regular data governance reporting.

13. Response Templates

The DPO maintains standard response letter templates for Subject Access Requests, erasure requests, and rectification requests. These templates are held within Annex A to this policy (section A8) and must be used as the basis for all formal responses, tailored to the specific circumstances of each case.

All SAR responses must include items (a) to (h) as set out in section 5.3 of this policy. Where the appropriate response is uncertain, the DPO must seek legal advice before responding.

14. Monitoring and Review

The DPO is responsible for monitoring compliance with this policy. The DPO must report on the volume and outcomes of individual data rights requests to the Operations Committee as part of regular data governance reporting.

This policy must be reviewed at least every two years, or earlier where required by changes in legislation, ICO guidance, or UKCBC's operational arrangements. Reviews must be conducted in accordance with GA 3.1 Policy Preparation and Version Control Guidance and the Review and Approval Framework.

Any member of staff who becomes aware of a failure to comply with this policy must report this to the DPO immediately. Where the DPO identifies a systemic or serious compliance failure that cannot be resolved operationally, the matter must be escalated to the Executive Leadership Team (ELT). The Board of Governors receives assurance on data governance and policy compliance through the Operations Committee's regular reporting.

15. Linked Policies

- DIG 2.1 Data Protection and Confidentiality Policy
- DIG 2.4 Records Management and Data Retention Policy
- SLCC 6.3 UKCBC Complaints Policy

16. External References

- UK General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018
- Freedom of Information Act 2000
- Information Commissioner's Office (ICO) — Subject Access Request guidance:

<https://www.ico.org.uk>

- ICO guidance on the right to erasure
- ICO guidance on the right to rectification
- UAE Federal Decree-Law No. 45 of 2021 on the Protection of Personal Data (UAE PDPL) (Dubai campus)

Appendix 1 — ICO Assurance Checklist

This checklist confirms that the policy addresses the key elements required by ICO guidance.

Requirement	Met?	Reference
Responsibilities clearly defined (who, what)	Yes	Section 4
Response timescales specified	Yes	Sections 5.4, 7, 8
Process for handling changes to data	Yes	Sections 7, 8
Process for rectification, erasure, and restriction	Yes	Sections 7, 8
Personal data accessible and filterable for SAR	Yes	Section 5.6
Staff training requirement stated	Yes	Section 4.1
List of relevant controllers and processors	Yes	Sections 3, 4
Exemptions identified and explained	Yes	Sections 6 and Annex A, Section 7
Record keeping requirements set out	Yes	Sections 12 and Annex A, Section 10
ICO complaint right included in responses	Yes	Sections 13 and Annex A, Section 8

Version History

Version	Date	Summary of Changes	Author	Approved By
v1.0	2018	Initial policy	Larry Gall	
v2.0	2020	Policy review and update	Ben Stedman	
v3.0	2022	Policy review; updated staff tables	Ben Stedman	
v4.0	March 2026	Full revision: updated to UK GDPR and DPA 2018; new Scope, Definitions, Exemptions, SAR Submission, Security and Retention, and Record Keeping sections added; step-by-step processes, identity verification list, response templates, and SITS checklist relocated to companion Procedure.	Pauline Williams	
v5.0	June 2026	Policy and Procedure combined into single document; companion Procedure (DIG 2.7-P) incorporated as Annex A; cross-references updated throughout; metadata updated; version numbering revised accordingly.	Pauline Williams	

Annex A

SAR and Individual Data Rights Procedure

This Annex forms part of DIG 2.7 Subject Access Request and Individual Data Rights Policy v5.0. It provides the operational steps, identification requirements, response templates, and system-specific guidance that the Data Protection Officer (DPO) and relevant staff must follow when handling individual data rights requests. The policy sets out UKCBC's legal obligations and governance framework. This Annex sets out how those obligations are discharged in practice.

This Annex must be read alongside the main policy. It applies to the DPO and to any member of staff instructed by the DPO to assist with an individual data rights request. It applies across all UKCBC locations, including the UK campuses and the Dubai campus.

All staff should be aware of sections A3.1 and A3.2, which set out what to do on first receipt of a request.

A3. Subject Access Requests — Step-by-Step Process

A3.1 Overview

A Subject Access Request (SAR) is a request by or on behalf of an individual for access to their personal data held by UKCBC. Any written or verbal request for personal data is likely to be a valid SAR, even if the individual does not use those words. On receipt, any member of staff must forward the request to the DPO immediately without assessment or response.

A3.2 Process

Step	Stage	Action	Notes
1	Request Received	Forward the request immediately to the DPO at dpo@ukcbc.ac.uk, regardless of the channel through which it was received.	Receipt of the request starts the statutory clock. The response deadline does not pause during College closure periods. All staff must recognise and forward requests without delay; a request does not need to use legal language to be valid.
2	Log Request	Enter the request in the Individual Data Request (IDR) register,	Account for College closure periods when calculating the

Step	Stage	Action	Notes
		recording: date of receipt; data subject name; requester name and address if different; type of data requested; and planned response date (no later than one calendar month from receipt).	response date. Ensure cover is in place to meet deadlines during planned closures.
3	Verify Identity	Verify the identity of the data subject. Where the request is made by a third party, verify both identities and the authority to act. See section A6 of this Annex for the accepted identification document list.	Do not release, erase, or correct any data until identity is verified. If verification cannot be completed, advise the data subject and document the reason.
4	Clarify Scope	Establish what information is being requested. Where the request is unclear, contact the data subject to clarify, but the statutory clock does not pause. Where the request overlaps with a FOIA request, treat each element under the applicable regime.	Requests submitted electronically should receive responses in electronic format wherever practicable.
5	Locate Data	Conduct a thorough search of all relevant systems, files, and data stores, including emails (including archived and recoverable deleted emails), documents, databases, CCTV footage, removable media, and paper records. Instruct all relevant departmental data owners in writing.	Do not alter, delete, or suppress any data identified during a SAR. Routine processing activities may continue.
6	Apply Exemptions	Review all responsive data for potential exemptions. Redact third-party personal data and any	Where uncertainty exists about whether an exemption applies,

Step	Stage	Action	Notes
		information covered by an applicable exemption. Document all redactions and the exemption applied. See section A7 of this Annex and section 6 of this policy.	seek DPO advice. Seek ICO guidance for complex cases.
7	Compile Response	Compile all disclosable information and prepare the response letter using the appropriate template from section A8 of this Annex. Ensure the response includes all required elements (a) to (h) as set out in section 5.3 of this policy.	Provide data in an intelligible form. Include explanations of codes, acronyms, and technical terms where needed.
8	Respond	Send the response within one calendar month of receipt. Where an extension is required for a complex request, notify the data subject within the first calendar month explaining the reason and confirming the revised deadline (maximum three months from receipt).	Responses must be free of charge unless the request is manifestly unfounded, excessive, or repetitive. Consult ICO guidance before applying this threshold.
9	Escalate Complaints	Where the data subject remains dissatisfied, manage the matter under the UKCBC Complaints Policy (SLCC 6.3) and advise the subject of their right to complain to the ICO at https://ico.org.uk or by telephone on 0303 123 1113.	Log the complaint outcome on the IDR register.

A4. Erasure Requests — Step-by-Step Process

A4.1 Overview

The right to erasure entitles individuals to request that UKCBC deletes their personal data in the circumstances set out in section 7 of this policy. The right is not absolute; certain data must be retained regardless of the request. Every erasure request must be assessed carefully and all retention decisions documented.

A4.2 Process

Step	Stage	Action	Notes
1	Request Received	Forward the request to the DPO at dpo@ukcbc.ac.uk immediately, regardless of the channel through which it was received.	Receipt starts the statutory clock. The one-calendar-month response deadline applies equally to erasure requests.
2	Log Request	Log the request on the IDR register.	Account for College closure periods when calculating the response date.
3	Verify Identity	Verify the identity of the data subject. See section A6 of this Annex for accepted identification documents.	Do not take any action on the request until identity is verified.
4	Check Scope	Search all relevant systems and data stores. Create a list of records subject to removal. Identify and document any data that must be retained, including qualification records, financial records, SFE records, and records subject to regulatory reporting or legal proceedings.	The right to erasure is not absolute. Document all retention decisions and the legal basis for each.

Step	Stage	Action	Notes
5	Send Initial Acknowledgement	Send the initial acknowledgement to the data subject (see template at section A8.2.1), confirming receipt, the records identified, and any data that will be retained.	Send acknowledgement promptly; do not wait until the process is complete.
6	Instruct Data Store Owners	Email all relevant departmental data owners providing subject identifiers and clear instructions on what must be deleted and what must be retained. Retain copies of all instructions sent.	Set a clear deadline for responses from data store owners. Two working days is recommended.
7	Chase Responses	Confirm that all data store owners have responded and confirmed completion. Chase non-responses within two working days. Where a data store owner remains unresponsive, escalate to the relevant departmental head. Where the matter cannot be resolved operationally, refer to the Executive Leadership Team (ELT).	Document all chase communications and escalation steps on the IDR register.
8	Send Completion Confirmation	Send the completion confirmation to the data subject (see template at section A8.2.2), confirming all data removed and any data retained with reasons.	Ensure the response is sent within one calendar month of receipt of the request.

A5. Rectification Requests — Step-by-Step Process

A5.1 Overview

The right to rectification entitles individuals to require UKCBC to correct inaccurate personal data held about them, or to complete incomplete data. This process must not be used to challenge academic results or decisions. It does apply where the outcome of a formal academic appeal has not yet been reflected on a student's record.

A5.2 Process

Step	Stage	Action	Notes
1	Request Received	Forward the request to the DPO at dpo@ukcbc.ac.uk immediately.	This process must not be used to challenge academic results or decisions. It does apply where the outcome of a formal academic appeal has not yet been reflected on a student's record.
2	Log Request	Log the request on the IDR register.	
3	Verify Identity	Verify the identity of the data subject. Where a third party is acting on the subject's behalf, verify both their identity and their authority to act. See section A6 of this Annex.	
4	Acknowledge Request	Send an initial acknowledgement to the data subject confirming receipt and the expected response timeline (one calendar month from receipt).	
5	Identify Records	Search all relevant systems and data stores to identify every record containing the data to be corrected.	

Step	Stage	Action	Notes
6	Obtain Evidence	Where data store owners require supporting evidence before making a correction, request this from the data subject and communicate the reason for the request.	Do not delay unnecessarily; the statutory clock continues to run.
7	Instruct Corrections	Email all relevant data store owners with clear instructions identifying what must be changed and what must remain. Confirm that no earlier version of the incorrect data can overwrite the correction.	Retain copies of all instructions sent.
8	Confirm Completion	Send the completion confirmation to the data subject (see template at section A8.3.1), confirming all corrections made.	

A6. Identity Verification — Accepted Documents

Before releasing, erasing, or correcting any personal data, the DPO must verify the identity of the data subject. Where a request is made by a third party, the DPO must verify both the third party's identity and their authority to act on the data subject's behalf.

UKCBC accepts the documents listed in the table below. Documents requiring currency must meet the time constraints specified.

Document	Currency Requirement
Current UK or international passport	None
UK Photocard Driving Licence (full or provisional)	None
EEA National Identity Card	None
Full UK Paper Driving Licence	None

Document	Currency Requirement
State Benefits Entitlement Document	Must be dated within the past 12 months
State Pension Entitlement Document	Must be dated within the past 12 months
HMRC Tax Credit Document	Must be dated within the past 12 months
Local Authority Benefit Document	Must be dated within the past 12 months
State or Local Authority Educational Grant Document	Must be dated within the past 12 months
HMRC Tax Notification Document	None
Disabled Driver's Pass	None
Financial Statement (bank, building society, or credit card company)	Must be dated within the past 3 months
Judiciary Document (Notice of Hearing, Summons, or Court Order)	None
Utility bill (gas, electricity, water, or telephone landline)	Must be dated within the past 3 months
Most recent Mortgage Statement	None
Most recent Council Tax Bill, Demand, or Statement	None
Current Council Rent Card or Council Tenancy Agreement	None
Building Society passbook showing a transaction within the past 3 months and current address	Must show transaction within the past 3 months

Where a data subject cannot provide acceptable identification, the DPO must advise on the appropriate course of action. No data must be released, erased, or corrected until identity is verified or the DPO has specifically authorised an alternative approach and documented the reason.

A7. Exemptions — Quick Reference

The full list of exemptions applicable to UKCBC is set out in section 6 of this policy. The table below provides a quick reference for operational use. Where uncertainty exists, the DPO must seek advice from the ICO before withholding data.

Exemption	When It May Apply	Action Required
Third-party personal data	Disclosure would reveal another individual's personal data without their consent.	Redact the third-party data and note the redaction.
Legal professional privilege	Data is covered by communications with UKCBC's legal advisers.	Seek legal advice before withholding.
Management forecasting	Data is processed for management forecasting or planning and disclosure would be likely to prejudice the conduct of UKCBC's business or activity. UKCBC must show the prejudice to the organisation outweighs the harm to the individual from being denied access.	Document the basis for applying the exemption. Apply on a case-by-case basis only.
Negotiations	Data records UKCBC's intentions in relation to negotiations with the data subject and disclosure would be likely to prejudice those negotiations. This exemption applies only whilst negotiations are ongoing.	Document the basis and stage of negotiations. Reassess if negotiations conclude before the request is responded to.
Crime and taxation	Disclosure would prejudice prevention or detection of crime or assessment of tax.	Seek DPO and, where appropriate, legal advice.

Exemption	When It May Apply	Action Required
Confidential references	References given or received in confidence for education, training, or employment.	Check whether consent to disclosure exists. Disclose if so.
Safeguarding and Prevent	Disclosure would prejudice safeguarding activities or Prevent duty obligations.	Seek DSL and DPO advice before responding.
Exam scripts	Data consists of examination scripts or examiner comments. Marks awarded are not exempt.	Redact scripts and comments; disclose marks.

Where data is withheld on the basis of an exemption, the DPO must document the exemption applied and inform the data subject that information has been withheld and the reason for this, unless doing so would itself undermine the purpose of the exemption.

A8. Response Templates

The templates below must be used as the basis for all formal responses to individual data rights requests. Each must be tailored to reflect the specific circumstances of the case. All templates must include items (a) to (h) as specified in section 5.3 of this policy, unless a specific exemption or circumstance applies.

Where the appropriate response is uncertain, the DPO must seek legal advice before responding.

A8.1 Subject Access Request Templates

A8.1.1 Full disclosure

(Name) (Address) (Date)

Dear (Name of data subject)

UK GDPR Subject Access Request

Thank you for your request of (date) for access to your personal data held by UK College of Business and Computing.

We are pleased to enclose the information you requested. [Include items (a) to (h) as set out in section 5.3 of this policy.]

Copyright in the information provided belongs to the College or to a third party. This material must not be copied, distributed, modified, reproduced, or published without the prior written consent of the copyright holder.

If you are not satisfied with our response, you have the right to complain to the Information Commissioner's Office (ICO) at ico.org.uk or by telephone on 0303 123 1113.

Yours sincerely

(Name) (Title) For the Data Protection Office, UKCBC

A8.1.2 Partial disclosure — information withheld under an exemption

(Name) (Address) (Date)

Dear (Name of data subject)

UK GDPR Subject Access Request

Thank you for your request of (date) for access to your personal data held by UK College of Business and Computing. To respond, we asked the following departments to search their records: (list departments).

We enclose (some / most) of the information you requested. Certain information has been redacted from the documents enclosed [or: We have not enclosed all of the information you requested]. This is because (explain the exemption that applies).

[Include items (a) to (h) as set out in section 5.3 of this policy.]

If you are not satisfied with our response, you have the right to complain to the ICO at ico.org.uk or by telephone on 0303 123 1113.

Yours sincerely

(Name) (Title) For the Data Protection Office, UKCBC

A8.1.3 No disclosure — all information withheld

(Name) (Address) (Date)

Dear (Name of data subject)

UK GDPR Subject Access Request

Thank you for your request of (date) for access to your personal data held by UK College of Business and Computing.

We regret that we are unable to provide the information you have requested. This is because (state reason / applicable exemption).

[Include items (a) to (h) as applicable.]

If you are not satisfied with our response, you have the right to complain to the ICO at ico.org.uk or by telephone on 0303 123 1113.

Yours sincerely

(Name) (Title) For the Data Protection Office, UKCBC

A8.1.4 Partial disclosure — confidential references

(Name) (Address) (Date)

Dear (Name of data subject)

UK GDPR Subject Access Request — References

Thank you for your request of (date) for access to references held by UK College of Business and Computing in connection with your (job / course) application.

We enclose (specify reference(s) that can be disclosed). We have not provided (a copy / copies) of (one / some) of the references you requested because (one of your referees / your referees) did not consent to disclosure.

[Include items (a) to (h) as set out in section 5.3 of this policy.]

If you are not satisfied with our response, you have the right to complain to the ICO at ico.org.uk or by telephone on 0303 123 1113.

Yours sincerely

(Name) (Title) For the Data Protection Office, UKCBC

A8.2 Erasure Request Templates

A8.2.1 Initial acknowledgement

(Name) (Address) (Date)

Dear (Name of data subject)

UK GDPR Right to Erasure Request — Acknowledgement

Thank you for your request of (date) for the removal of your personal data from the records of UK College of Business and Computing.

We are now progressing your request and will contact you once it is complete. We have identified the following records relating to you: (list records). We will ensure that all data we are able to erase is removed from both digital and paper records.

Please note that we are required by law to retain certain records, including those relating to qualifications obtained, financial transactions, and obligations to government bodies such as Student Finance England. We will inform you of any data we are unable to erase.

Yours sincerely

(Name) (Title) For the Data Protection Office, UKCBC

A8.2.2 Completion confirmation

(Name) (Address) (Date)

Dear (Name of data subject)

UK GDPR Right to Erasure Request — Completion

We write further to your request of (date) for the removal of your personal data from our records. We can confirm that all data we were able to erase, including both paper and digital records, has now been removed, subject to the exclusions below.

Retained data: (Describe the data retained and the legal basis for retention, e.g. records relating to a qualification obtained; records relating to a funding arrangement with Student Finance England.)

If you are not satisfied with our response, you have the right to complain to the ICO at ico.org.uk or by telephone on 0303 123 1113.

Yours sincerely

(Name) (Title) For the Data Protection Office, UKCBC

A8.3 Rectification Request Templates

A8.3.1 Completion confirmation

(Name) (Address) (Date)

Dear (Name of data subject)

UK GDPR Right to Rectification — Completion

We write further to your request of (date) for correction of your personal data held by UK College of Business and Computing.

We can confirm that the following corrections have been made to your records: (describe corrections made). We have verified that no earlier version of the incorrect data remains in any system that could overwrite the correction.

If you are not satisfied with our response, you have the right to complain to the ICO at ico.org.uk or by telephone on 0303 123 1113.

Yours sincerely

(Name) (Title) For the Data Protection Office, UKCBC

A9. SITS Removal Checklist for Students

This checklist must be completed by the relevant data store owner when processing an erasure request for a student or former student. It must be returned to the DPO with confirmation of completion. Retain a copy on the IDR register file for the request.

Area	Search By	Data to Remove	Completed
Master Person	ID and Name	Confirm no duplicate records exist under another ID. Check all marketing communications preferences are set to N and no active consent records remain.	
Prospects	ID	Remove all prospect records where no retention obligation applies.	
Admissions	ID	Remove: addresses, interview details, employment information, additional personal details, documents, and processing logs.	
Student Records	ID	Remove: authorised absence records, next of kin details, documents, attendance and absence records, and incident records.	
General Applicant / Student	ID	Remove: workflow logs and GSL communications records.	

A10. Record Keeping

The DPO must maintain the IDR register in accordance with section 12 of this policy. A record must be created for every individual data rights request received, regardless of the outcome.

SAR-related records, including logs, correspondence, and response documentation, must be retained for two to three years from the date on which the request is closed, in accordance with sections 11.2 and 12.2 of this policy. On expiry of the retention period, all materials must be disposed of securely: electronic files must be permanently deleted and paper documents must be shredded or disposed of via a secure waste service. Disposal must be recorded on the IDR register.

A11. Monitoring and Review

The DPO is responsible for maintaining this Annex and ensuring it remains accurate and operationally effective. This Annex must be reviewed at the same time as the main policy, at least every two years, or earlier where required by changes in legislation, ICO guidance, or UKCBC's systems and processes.

The DPO must report on the volume and outcomes of individual data rights requests to the Operations Committee as part of regular data governance reporting.

A12. Linked Documents

- DIG 2.7 Subject Access Request and Individual Data Rights Policy (main policy, of which this is Annex A)
- DIG 2.1 Data Protection and Confidentiality Policy
- SLCC 6.3 UKCBC Complaints Policy

Annex A — Version History

Version	Date	Summary	Author	Approved By
v1.0	May 2026	Initial procedure. Operational content relocated from DIG 2.7 policy; step-by-step processes, identity verification list, sample letters, and SITS removal checklist consolidated here.	Pauline Williams	
v2.0	June 2026	Procedure incorporated as Annex A to DIG 2.7 v5.0. Cross-references updated to align with revised policy section numbering.	Pauline Williams	