

IBCM Data Protection Policy

1.0 Introduction and Purpose

As part of the general operation of our business, International Business College Manchester (IBCM) will at certain times create and obtain data relating to finances, holdings, clients, staff and business arrangements. It is vital that all such data collection, management and storage be handled in a manner that adheres to relevant laws and charters and reflects IBCM commitment to corporate responsibility in this area.

IBCM's reputation and future growth are dependent on the way the College manages and protects personal data. Protecting the confidentiality and integrity of personal data is a key responsibility of everyone within the College.

As an organisation that collects, uses and stores personal data about its employees, suppliers, students governors and visitors, the College recognises that having controls around the collection, use, retention and destruction of personal data is important in order to comply with the College's obligations under the Data Protection Laws and in particular its obligations under Article 5 of UK GDPR.

IBCM is not of sufficient scale that a Data Protection Office DPO is appropriate. In each team – Admin, Finances, Marketing and Academic, the manager will be responsible reporting to the MD. Record keeping, documentation, processes, audits and reviews must demonstrate adherence to IBCM policies and accountability in this regard.

This policy is intended to ensure that personal information is dealt with correctly and securely and in accordance with the UK General Data Protection Regulations (UKGDPR). It will apply to all information regardless of the way it is collected, used, recorded, stored and destroyed, and irrespective of whether it is held in paper files or electronically. All staff involved with the collection, processing and disclosure of personal data will be aware of their duties and responsibilities by adhering to these guidelines.

2.0 Scope

2.1 This policy applies to:

- All personal data created or received in the course of college business in all formats, of any age. "Personal Data" shall include personal and special category data.
- Personal data held or transmitted in physical (including paper) and electronic formats
- Personal data transmitted in verbal format (e.g. in conversation, in a meeting, or over the telephone)

2.2 Who is affected by the policy:

- College staff (including contractors, temporary staff and anyone else who can access or use personal data, including special categories of data, in their work for the College)

- Non-staff data subjects (these include, but are not confined to: prospective applicants; applicants to programmes and posts; current and former students; former employees; family members where emergency or next of kin contacts are held; customers, people making requests for information or enquiries professional contacts)

2.3 Where the policy applies:

- This policy applies to all locations from which college data is accessed, including home access and overseas.

3.0 Personal Data

Personal Data in our context refers to items such as:

Name, age, location data, online identifiers, qualifications, background information, factors relating to the physiological, mental, genetic, socio-economic, financial, gender identification, health, cultural and social identity of the individuals.

We will be required to store and to process data about:

- current, past and prospective students
- current and former staff
- homestay hosts and their families including other residents in their homes

Every effort will be taken to ensure that the collection of data in relation to the above is limited to that necessary for IBCM to perform efficiently in the following explicit and legitimate areas:

- the functions of arranging student accommodation and transfers,
- classes, examinations and academic record keeping,
- financial operations and invoicing
- recruitment and staffing

4.0 Definition of Terms

- **Data subject** – all living individuals about whom we hold data
- **Data** – any stored information (whether electronic or paper)
- **Personal data** – data relating to a living individual who can be identified from that data. It can be factual or opinion based. The UKGDPR applies to ‘personal data’ meaning any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier. This definition provides for a wide range of personal identifiers to constitute personal data, including name, identification number, location data or online identifier, reflecting changes in technology and the way organisations collect information about people.
- **Special categories of personal data** – this would include information about a person’s racial or ethnic origin, political opinions, religious beliefs, physical health, mental health, sexual orientation, criminal record. *The processing of such data may only be done under strict conditions and requires the explicit and informed consent of the individual concerned.*
- **Data controller** - a person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be processed

- **Data processor** - in relation to personal data, means any person (other than an employee of the data controller) who processes the data on behalf of the data controller.
- **Processing** - in relation to information or data means obtaining, recording or holding the information or data or carrying out any operation or set of operations on the information or data, including—
 - a) organisation, adaptation or alteration of the information or data,
 - b) retrieval, consultation or use of the information or data,
 - c) disclosure of the information or data by transmission, dissemination or otherwise making it available to a third party

5.0 Data Protection Principles

IBCM will adhere to the following basic principles of data protection

5.1 Principle 1: Personal data shall be processed fairly, lawfully and transparently:

- Individual has given consent for the use of their data for one or more specific purposes
- Processing is necessary for the performance of a contract between IBCM and the individual/organisation
- Processing is necessary for compliance with IBCM compliance with legal obligations
- Processing is necessary to protect the vital interests of the individual
- People are informed about how we use their personal data and what their rights are.

5.2 Principle 2: Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner incompatible with those purposes:

- The use of data collected for one purpose should be limited to that particular purpose.
- Where student data is requested for marketing purposes, written permission will be obtained first. Lack of response/no visible objection will not be taken as consent.
- Be clear in the privacy notice as to the specific purposes of processing and ensure the data subjects are fully informed.

5.3 Principle 3: Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed (data minimisation):

- Only the minimum data required will be collected
- Where possible personal data will be anonymised
- Data will be reviewed periodically and where appropriate data will be deleted when not needed.

5.4 Principle 4: Personal data shall be accurate and, where necessary, kept up to date every reasonable step must be taken to ensure personal data that is inaccurate is erased or rectified without delay (accuracy)

- All reasonable steps will be taken to ensure personal data is not incorrect and have processes in place to ensure incorrect or misleading data is corrected or erased

- ensure accuracy of personal data we create and record the source of the data
- Have processes in place to address and individual's right to rectification; how it is considered actioned and recorded.

5.5 Principle 5: Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed (storage limitation):

- Personal data will only be kept for as long as necessary and only for the purpose it was collected for
- Processes will be in place to comply with individuals requests for erasure under the “right to be forgotten”
- Personal data will be destroyed securely in a manner appropriate to its format

5.6 Principle 6: Personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction, or damage, using appropriate technical or organisational measures (Security)

- Appropriate organisational, technical and physical security measures to be in place to protect personal data with appropriate training, monitoring and control measures.

6.0 Rights of data subjects

Individuals have rights under data protection law.

6.1 Right to be informed

Individuals have the right to be informed about the collection and use of their personal data. This is a key transparency requirement under the UKGDPR. We will provide individuals with information including: our purposes for processing their personal data, our retention periods for that personal data, and who it will be shared with. This is called ‘privacy information’. We will provide privacy information to individuals at the time we collect their personal data from them. If we obtain personal data from other sources, we will provide individuals with privacy information within a reasonable period of obtaining the data and no later than one month. The information we provide to people will be concise, transparent, intelligible, easily accessible, and it will use clear and plain language. We will bring any new uses of an individual’s personal data to their attention before we start the processing.

6.2 Right of access

Individuals have the right to access their personal data and supplementary information without charge. The right of access allows individuals to be aware of and verify the lawfulness of the processing. If data subjects want access to their data, in the first instance they should contact the principal of the college.

6.3 Right of rectification of data

Individuals have the right to have inaccurate personal data rectified and incomplete personal data completed.

6.4 Right to erasure

The right to erasure is also known as 'the right to be forgotten'. This means that individuals can request the deletion or removal of personal data when it is no longer needed, if the data has been unlawfully processed, or if the data subject withdraws their consent, unless there is an overriding legal or public interest in continuing to process the data.

6.5 Right to restrict processing

Individuals have a right to 'block' or suppress processing of personal data until a dispute about the data's accuracy or use has been resolved, or when the College no longer needs to keep personal data but the data subject needs the data for a legal claim.

6.6 Right to portability

The right to data portability allows individuals to obtain and reuse their personal data for their own purposes across different services. It allows them to move, copy or transfer personal data easily from one IT environment to another in a safe and secure way, without hindrance to usability.

6.7 The right to object

All individuals have the right to object and prevent further processing of their data in certain circumstances, including where the College is:

- Processing personal data for direct marketing
- Processing data obtained for online service such as social media, where consent for the processing was previously given by or on behalf of a child who withdraws their consent
- Making a decision about them taken solely by automated means
- Carrying out processing in the course of the College's legitimate interest or public interest unless the College can demonstrate compelling lawful grounds for continuing to process the individuals data

6.8 Rights in relation to automated decision-making and profiling

Automated decision making means a decision is made solely by automated means and without any human intervention. Profiling is automated processing of personal data to evaluate certain things about an individual. Profiling can be part of an automated decision-making process. This type of decision making can only be carried out where the decision is necessary for the entry into or performance of a contract; authorised by law or based on the individual's explicit consent. When the College processes personal data which involves automated decision making or profiling, the College will provide the individual with information about the processing and provide a simple way for them to request human intervention or challenge a decision.

7.0 Data Breach

- A personal data breach is defined as:
a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed
- Upon becoming aware of any such breach, notification must be made to the relevant Data Protection Commissioner within 72 hours.
- Report should be made by the local Data Compliance Officer and must identify the likely consequences of the breach and the measures taken/to be taken to mitigate possible adverse effects for individuals.
- Facts surrounding the breach, its effects, remedial action taken must be documented to verify compliance.
- Individuals must be notified if the breach is likely to result in high risk for their rights and freedoms

8.0 Practical Considerations

- IBCM operates a Clean Desk Policy. All documents of a sensitive/restricted or personal nature are to be tidied away and either securely disposed of or locked away when the workspace is not occupied. This includes Post-Its and memos.
- File cabinets containing Restricted or Sensitive information must be kept closed and locked when not in use or when not attended.
- Keys used for access to Restricted or Sensitive information must not be left at an unattended desk.
- All IBCM computers are timed to lock automatically at 5 minutes. All IBCM computers require a password to access.
- Those leaving their desk or workspace are required to manually lock their computer as follows:
- Computer workstations must be shut down at the end of the day.

Policy version	V 1.0 2024_2025 June 2024
Originator	Academic & Quality Manager
Effective From	June 2024
Approved by	Executive Committee
Date of review	July 2025

Appendix 1

Document Retention by Years

1 YEAR

Correspondence with Customers and Vendors
Duplicate Deposit Slips
Purchase Orders (other than Purchasing Department copy)
Receiving Sheets
Requisitions
Stockroom Withdrawal Forms

3 YEARS

Class/academic records
Employee Personnel Records (after termination)
Employment Applications
Expired Insurance Policies
General Correspondence
Internal Audit Reports
Internal Reports
Petty Cash Vouchers
Physical Inventory Tags

6 YEARS

Accident Reports, Claims
Accounts Payable Ledgers and Schedules
Accounts Receivable Ledgers and Schedules
Bank Statements and Reconciliations
Cancelled Checks
Employment Tax Records
Expense Analysis and Expense Distribution Schedules
Expired Contracts, Leases
Inventories of Products, Materials, Supplies
Invoices to Customers
Notes Receivable Ledgers, Schedules

Payroll Records and Summaries, including payment to pensioners
Purchasing Department Copies of Purchase Orders
Sales Records
Subsidiary Ledgers
Time Books
Travel and Entertainment Records
Vouchers for Payments to Vendors,
Employees, etc. Voucher Register,
Schedules

FOREVER

Audit Reports from CPAs/Accountants
Cancelled Checks for Important Payments (especially tax payments)
Cash Books, Charts of Accounts
Contracts, Leases Currently in Effect
Corporate Documents (incorporation, charter, by-laws, etc.)
Documents substantiating fixed asset additions
Deeds
Depreciation Schedules
Financial Statements (Year End)
General and Private Ledgers, Year End Trial Balances
Insurance Records, Current Accident Reports, Claims, Policies
Investment Trade Confirmations
IRS Revenue Agents. Reports
Journals
Legal Records, Correspondence and Other Important Matters
Minutes Books of Directors and Stockholders
Mortgages, Bills of Sale
Property Appraisals by Outside Appraisers
Property Records
Retirement and Pension Records
Tax Returns and Worksheets
Trademark and Patent Registrations

Digital academic records

Digital records of certification and examination results

PRIVACY NOTICE FOR STAFF AND HOMESTAY HOSTS

YOUR PERSONAL INFORMATION AND HOW WE USE IT

IBCM will collect and use personal information about you (our staff and homestay hosts). We do this through the completion of various forms which ask for your personal details

We hold and use your information to help us fulfil our contractual obligations to you (i.e. to pay you) and to help us provide a safe and secure environment for you to work in. We also use the information in order to ensure that we all have a safe and secure environment for our students (i.e. by asking you to undertake DBS checks)

The information we hold includes (but is not necessarily limited to) your

- personal contact details
- banking details
- evidence of DBS clearance
- information about your family home (in the case of homestay hosts) □ educational qualifications

We will hold all of your personal information securely and only those with a legitimate need to access it will be permitted to. We will not pass any personal information on to third parties unless we have received your **explicit written consent** to do so.

You can ask to see any information we hold about you.

There is no cost to see this information

You can see the full IBCM Data Protection Policy here by looking on our website or by contacting the Principal

If you have any questions about the way we use your personal data, contact enquires@ibc-manchester.com

PRIVACY NOTICE FOR STUDENTS

YOUR PERSONAL INFORMATION AND HOW WE USE IT

IBCM will collect and use personal information about you (our students). We will ask you to complete forms giving us your personal details in case there is an emergency and we need to contact you or someone in your family.

We hold and use your information to help you study and learn, to check and to report on how well you are doing and to make sure you are happy and safe with us.

The information we hold includes your

- contact details
- attendance information
- special educational needs and
- any important medical information

We will give important medical information to your homestay host and to other IBCM staff members.

We will also give your contact details to homestay hosts and to other IBCM staff members. We do this for your health and for your safety.

You can ask to see any information we hold about you. Just ask the Principal. There is no cost to see this information

If you want to see our full Data Protection Policy please look on our website or ask the Principal of your school

If you have any questions about the way we use your personal data, contact enquiries@ibc-manchester.com

Appendix 4

Data Breach Notification Form *How*

to complete this form:

This Form is in two sections. Section 1 covers the initial information which must be notified to this Office in respect of a data security breach, and Section 2 requests more detailed further information.

A first notification must be made to this Office on this form no later than 24 hours after the first detection of the data breach.

If you have all the information to hand at this stage, you may fill out both sections 1 and 2 of the form.

If you do not have all the necessary information to hand at the time of the first notification, a second notification must be made within 3 days of the first notification, on section 2 of the form. For security purposes, you will not be presented with the information previously supplied in Section 1. When submitting a second notification, please complete Questions 1-3 again and Questions 4-8 if there is any change to the information. If there is no change to your responses to questions 4 to 8 from your initial notification, simply enter "as initial notification".

If at the end of the 3 days, you still do not have all the information required, you must provide as much information as is available and contact:

Ireland: the Data Breach Section of the Office of the Data Protection Commissioner to provide a reasoned justification for the late notification of the remaining information. The Breach section can be contacted on (057) 8684800.

UK: the Data Breach Section of the Information Commissioner's Office. The Breach section can be contacted on 0303 123 1113. The relevant web site may be accessed via <https://ico.org.uk/for-organisations/report-a-breach/> SECTION

1

Information in this section is for an initial notification. Preliminary information is sufficient for answers in this section.

Questions 1 and 2

1. Name of the provider and
2. Contact details as indicated.

Question 3

Please indicate whether or not you are making a first or second notification.

You will receive a reference number from this Office when you make your first notification. If you are subsequently making a second notification, please include the reference number here.

Question 4

Please indicate both the date and time when the incident took place and the date and time when the incident was detected by the provider.

Question 5

Please indicate the circumstances surrounding the breach.

Question 6

Please indicate the nature and content of the personal data

Question 7

Please indicate the technical and organisational measures you are applying to secure the affected data.

Question 8

Please indicate if you use other providers to deliver part of the electronic communications service to your subscribers. If the breach was related to the service provided by these other providers, please indicate if they notified you of the data security breach.

At the end of Section 1 you will be given an option either to submit the form as an initial notification or to proceed to section 2 to make a full notification, if you have the information available to you at this time.

If you submit you will receive an automated email as an initial acknowledgment. SECTION

2

Further Information on the data breach.

Question 9

Please give a summary of the incident that caused the data breach, including the physical location and the storage media involved.

Question 10

Please indicate the number of subscribers or individuals concerned.

Question 11

Please describe the potential consequences and potential adverse effects on subscribers/individuals.

Question 12

Please describe what action you have taken to help mitigate any potential adverse affects to the affected individuals.

Possible additional notification to subscribers/individuals

Question 13

If you have already notified subscribers/individuals, please give the content of the notification.

Question 14

If you have already notified subscribers/individuals, please indicate the means used to notify the breach to subscribers/individuals (e.g. individual notifications- email, letter or phone call, media announcements etc) Question

15

Please indicate the number of subscribers/individuals notified.

Possible cross-border issues

Question 16

Please indicate if the breach has involved subscribers/individuals in other Member States Question

17

Please indicate if you have notified other competent national authorities.

If you have notified other competent national authorities, please indicate which authorities you have notified.