INTERNATIONAL FOUNDATION GROUP

051. Data Management and Protection Policy

Policy owner:	**Marketing & Partnerships Director (Data Protection Lead)**
Version No.:	**2.0**
Review cycle:	**Annually**
Approval route:	**Operations Board**
Publication route:	**External (IFG website)**
Latest publication date:	**13.02.2026**

Introduction

IFG's ICO Registration: ZB018036

International Foundation Group (IFG), through the nature of its business, sometimes has to deal with personal and/or potentially sensitive data. This data may be from students, applicants, employees or other organisations and may be in the form of personal or contact details, employment and educational histories, and other types of personal data appropriate to the nature of our organisation and activities.

The law in the UK relating to processing data is called the Data Protection Act (2018) and is in line with the UK General Data Protection Regulations (GDPR 2018). This legislation places obligations on all organisations that process personal information and gives individuals certain rights.

Data Protection and Processing Principles

Article 5 of the UK GDPR sets out the seven core principles of personal data processing.. In practice, these principles function as the requirements IFG measures itself against to ensure compliant processing. The seven principles are:

1. Lawfulness, fairness and transparency
    - Have a valid lawful basis for every use of personal data, do nothing illegal with it, and avoid uses that people would not reasonably expect.
    - Be open by providing clear privacy information about what you collect, why and how it will be used.
2. Purpose limitation
    - Collect data only for specified, explicit and legitimate purposes stated at the outset.
    - Do not repurpose it in ways that are incompatible with those original purposes unless you have a new lawful basis (or as a specific legal provision allowing this).
3. Data minimisation
    - Collect and keep only the personal data that is genuinely necessary for the stated purposes.

    - Ensure the data is adequate, relevant and limited to what is necessary, rather than collecting 'just in case' information.
4. Accuracy
    - Take reasonable steps to ensure personal data is accurate and, where necessary, kept up to date.
    - Correct or delete inaccurate or misleading data without undue delay when you become aware of it.
5. Storage limitation
    - Keep personal data in identifiable form no longer than is necessary for the purposes for which it was collected.
    - Set and apply retention periods and securely delete or anonymise data once it is no longer needed.
6. Integrity and confidentiality (security)
    - Protect personal data against unauthorised or unlawful processing and against accidental loss, destruction or damage.
    - Use appropriate technical and organisational measures (access controls, encryption, policies, training etc.) proportionate to the risks.
7. Accountability
    - Be able to demonstrate compliance with all of the above principles (eg via policies, DPIAs, records of processing, training and audits).
    - Embed data protection governance so that responsibility and decision-making are clear and documented.

The UK GDPR and DPA (2018) apply to data controllers (who decide the purposes and means of processing) and data processors (who handle data on behalf of data controllers). They cover the collection and processing of personal data of living individuals (for example, names, household addresses, telephone numbers, email addresses, IP addresses, location data and other personal information).

Lawful bases for processing personal data

Under the UK GDPR, as a Data Controller, IFG must identify one or more of the six lawful bases for processing data. The six lawful bases are:

- **Consent:** The data subject has given clear consent for the controller to process their personal data for one or more specific purposes.
- **Contract:** Processing is necessary for the performance of a contract with the data subject, or to take steps at their request before entering a contract.
- **Legal obligation:** Processing is necessary for compliance with a legal obligation to which the controller is subject.
- **Vital interests:** Processing is necessary to protect the vital interests of the data subject or another natural person.
- **Public task:** Processing is necessary for the performance of a task carried out in the public interest, or in the exercise of official authority vested in the controller.
- **Legitimate interests:** Processing is necessary for the purposes of the legitimate interests pursued by the controller or a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject.

Information Commissioner's Office (ICO)

Under UK law, all individuals and companies who store and process information and personal data are required to register themselves as Data Controllers with the Information Commissioner's Office (ICO). This process is called notification and requires data controllers to list the types of data they process and the reasons they process that data. This information is then made available to the public for inspection via a public register. The main purpose of notification and the public register is to promote openness in the use of personal information. Notification helps us, as a company, to be transparent and open about how and why we process data and helps our clients, students, parents, suppliers, alumni and staff to understand how their personal information is being processed.

"International Foundation Group (IFG) is registered with the Information Commissioner's Office (ICO) as a Data Controller. As an organisation, we are committed to the highest standards of privacy and have therefore created a position of Data Protection Lead, held by the Marketing and Partnerships Director. This commitment, endorsed by our Academic Director/CEO, signifies IFG's senior-level accountability toward data protection and that IFG adheres to procedures in order to safeguard the personal information of our students, staff, and partners."

Aim of this Policy

The aim of this data protection policy is to set out simply and clearly the obligations and commitments of the International Foundation Group (IFG), its students and employees with regards to processing personal data. This policy is an extension of International Foundation Group (IFG)'s legal requirements, which are covered in detail in the General Data Protection Regulations. Details of legal requirements along with relevant statutory guidance regarding data protection can be found at www.ico.gov.uk.

What data IFG processes

APPLICANT and STUDENT DATA

Please see Appendix C to this policy, Procedure for Creating and Monitoring Student Records, which covers IFG's operation and management of the following areas regarding student data.

IFG obtains or receives personal data about applicants and students from the following:

- When contact details are given to us to register for for open day or other IFG admissions/recruitment activities
- When further information is requested from us regarding an admissions or other student-related enquiry
- When an individual makes an application for an IFG course
- When an individual registers as a student on an IFG course
- From third party sources (such as other institutions involved in the delivery of joint programmes, Government Departments such as the Home Office or the Student Loans Company, or other individuals such as Schools and Colleges)
- From applicants and students when they disclose personal data during the course of their studies or when accessing our services or resources (e.g. careers advice, counselling, financial support);

Personal Data collected and processed

Personal Data collected and processed via the above mechanisms and sources includes:

1. **Applicant data**

- Contact details (eg name, address, email, phone)
- Equality Monitoring Data (eg ethnicity, sex/gender, age, disability, sexual orientation)
- Educational history (eg prior qualifications, UCAS personal ID),
- Socioeconomic indicators (eg POLAR quintile, IMD from postcode, free school meals historical eligibility)
- Equality of Access data (eg care experience, estrangement, Gypsy/Roma status)
- Personal identifiers (eg passport details, nationality, date of birth)
- English language competency (eg IELTS/SELTS results)
- Financial data (eg household income, proof of funds for Student Visa purposes)
- Student Visa-related information (eg scholarship/sponsor details, visa-compliance history)

2. **Student Enrolment data**
   - Student identifiers (student number we assign, date of birth, nationality, domicile)
   - Demographic details (mirroring applicant data plus next of kin/trusted contact, marital status and any relevant details applicable to our Personal Relationships Policy)
   - Course-related information (mode of study, qualification aim, funding category)
   - Support/other specific needs (disability adjustments, safeguarding considerations, initial arrangements under Support Through Studies framework)
   - Medical information and form

3. **Engagement and Outcomes Data (ongoing processing)**
   - Attendance and engagement instances (records of attendance at scheduled lectures/seminars/classes, examinations attendance, summative assessment submissions)
   - Engagement matters (extenuating circumstances applications and reasons,
   - Assessment results and related information (provisional and confirmed results, and related academic feedback, of all summative assessments, results and feedback of formative assessments, records of academic appeal submissions and outcomes)
   - Other student-related matters (academic misconduct records and outcomes, non-academic misconduct records and outcomes, records and outcomes relating to other IFG student-related processes such as Initial Investigations under the Policy on Sexual Misconduct, Harassment & Unacceptable Behaviours)

Formats of personal data collected and processed

- Electronic and hard copy documentary student records (including registration records and application forms; documents generated by academic/casework activities etc.)
- Statistical and demographic data either collected by IFG or provided to IFG eg by the Office for Students/HESA, Student Funding Bodies;
- Photographic images; audio, visual and audio-visual recordings (e.g. of classes, seminars, lectures, performances, assessments, and other learning activities)
- Work produced by students in the course of their studies, including written, practical, audiovisual, and/or recorded work, and examination scripts.

OTHER PERSONAL DATA

International Foundation Group (IFG) processes personal data as a necessary part of business activities. Any personal data that the company, or an individual acting on behalf of the company collects, stores or processes in any way, whether on a computer or on paper, will have appropriate safeguards applied to it to ensure that International Foundation Group (IFG) complies with its lawful obligations.

International Foundation Group (IFG) is registered with the Information Commissioner's Office as a Data Controller, allowing it to process personal information for various purposes. International Foundation Group (IFG) will only collect Data for the sole purpose of meeting specifically planned, agreed and necessary purposes and will retain that information as long as those purposes remain valid. These purposes currently include:

Staff administration including, but not limited to: appointments or removals, pay, discipline, superannuation, work management or other personnel matters in relation to its staff.

Advertising Marketing and Public Relations including, but not limited to: advertising or marketing the business activity, goods or services and promoting public relations in connection with that business or activity, or those goods or services.

Accounts and Financial Records including, but not limited to: keeping accounts related to any business or other activity carried on by the data controller, or deciding whether to accept any person as a customer or supplier, or keeping records of purchases, sales or other transactions for the purpose of ensuring that the requisite payments and deliveries are made or services provided by him or to him in respect of those transactions, or for the purpose of making financial or management forecasts to assist him in the conduct of any such business or activity.

Consultancy or Advisory Services including, but not limited to: giving advice or rendering professional services, the provision of services of an advisory, consultancy or intermediary nature.

Any personal data collected by International Foundation Group (IFG) will only be passed to a third party where required by law, to comply with a statutory obligation or where International Foundation Group (IFG) has obtained the express written consent of the individual concerned or where the information held on a student who is under the age of 18, by their parent or guardian.

How IFG manages data

In accordance with its duty to comply with the Data Protection Principles, International Foundation Group (IFG) will:

- Ensure that all data processed is done so fairly and under both the letter and the spirit of the law;
- Clearly identify the applicable lawful basis in accordance with UK GDPR (2018) Article 6 and record the specific purposes under which International Foundation Group (IFG) will process data;
- Ensure that data collected and processed only to the extent that it is needed to fulfil operational needs or to comply with any legal requirements;
- Ensure that data is true and meaningful and regularly updated;
- Ensure that data is never held for longer than is required;
- Process data in such a way that the rights of individuals under the Act are easily and swiftly exercised;
- Take appropriate physical and electronic safety measures in order to safeguard the data;
- Never transfer personal information to countries which do not have a similar or equivalent policy or similar safeguarding process for personal data.

As the nature of International Foundation Group (IFG)'s business means that it may, from time to time, process sensitive personal information about an individual. On such occasions, International Foundation Group (IFG) will ensure that it has explicit consent to hold, use and retain such data regarding the individual.

Sensitive personal data (Special Category Data)

Under Article 9 of the UK GDPR, sensitive personal data (referred to as special category data) may include: personal data about an individual's racial or ethnic origin, political opinions, religious beliefs, trade union membership, physical or mental health, or sexual orientation. Article 9 sets out both the definition of special category data and the conditions under which it can be processed lawfully in addition to having a lawful basis under Article 6. There are 10 conditions under Article 9 permitting the processing of special category data (in addition to an Article 6 lawful basis), which are:

(a) Explicit consent: The data subject has given explicit consent for one or more specified purposes, except where UK law provides a safeguard for the data subject's rights and freedoms.

(b) Employment, social security and social protection: Processing is necessary for carrying out obligations or rights of the controller or data subject under employment, social security, or social protection law, authorised by UK law with appropriate safeguards.

(c) Vital interests: Processing is necessary to protect the vital interests of the data subject or another where they are physically or legally incapable of giving consent.

(d) Not-for-profit bodies: Processing is carried out by a not-for-profit body with a political, philosophical, religious, or trade union aim, subject to conditions protecting data subjects' interests.

(e) Made public by data subject: Processing relates to personal data manifestly made public by the data subject.

(f) Legal claims or judicial acts: Processing is necessary for establishing, exercising, or defending legal claims, or where courts act in their judicial capacity.

(g) Substantial public interest: Processing is necessary for reasons of substantial public interest, based on UK law proportionate to the aim with suitable safeguards.

(h) Health or social care: Processing is necessary for preventive/occupational medicine, assessing working capacity, medical diagnosis, health/social care provision, or management, authorised by UK law or health professional contract.

(i) Public health: Processing is necessary for public health reasons (e.g., ensuring high-quality healthcare), authorised by UK law with safeguards like professional secrecy.

(j) Archiving, research, statistics: Processing is necessary for archiving in the public interest, scientific/historical research, or statistics per Article 89(1), based on proportionate UK law.

Data about criminal offence allegations or convictions, which includes details of the commitment or alleged commitment of any offence and any court proceedings relating to the commission of an offence, is also classified as sensitive personal data but is governed under Article 10 of the UK GDPR. Article 10 requires IFG to identify both a lawful basis and a condition from Schedule 1 of the DPA 2018 (such conditions are usually found in Parts 2 or 3 of Schedule 1), plus an appropriate policy document must be maintained for accountability purposes (please see the IFG Criminal Records Policy).

Data Breach Notification

Where a Data Breach is likely to result in a risk to the rights and freedoms of the individual(s) concerned, we will report it to the Information Commissioner's Office within 72 hours of us becoming aware of it, and it may be reported in more than one instalment.

Individuals will be informed directly if the breach is likely to result in a high risk to their rights and freedoms.

If the breach is sufficient to warrant notification to the public, we will do so without undue delay.

If you know or suspect that a Data Breach has occurred, do not attempt to investigate the matter yourself but contact your manager or the IFG Data Controller immediately, preserving all evidence relating to the potential data breach.

Data Subject's Rights and Requests

Under data protection law, you have a number of rights over your personal information, including:

- *Your right of access:* You have the right to ask us for copies of your personal information.
- *Your right to rectification:* You have the right to ask us to rectify personal information you think is inaccurate. You also have the right to ask us to complete information you think is incomplete.
- *Your right to erasure:* You have the right to ask us to erase your personal information in certain circumstances.
- *Your right to restriction of processing:* You have the right to ask us to restrict the processing of your personal information in certain circumstances.
- *Your right to object to processing*: You have the right to object to the processing of your personal information in certain circumstances.
- *Your right to data portability:* You have the right to ask that we transfer the personal information you gave us to another organisation, or to you, in certain circumstances.

You can exercise these rights by contacting the IFG's Data Protection Lead via email on: s.green@intfoundationgroup.co.uk. In some instances, you may make a Subject Access Request (see below). You are not required to pay any charge for exercising your rights. If you make a request to exercise any of the above rights, IFG has one month to respond to you.

Subject Access Requests

Under the General Data Protection Regulation, individuals have a right to obtain a copy of personal information held about them on computers and in some manual filing systems. This is known as the right of subject access. Subject access requests must be requested in writing and IFG must process them within 40 days, although International Foundation Group (IFG) has the right to request any information they reasonably require to find the information and check the identity of the individual making the inquiry.

IFG does not charge a fee for Subject Access Requests. If the details held about you are inaccurate, you have the right to ask the IFG to correct, rectify, block or erase such inaccurate information. In certain circumstances you may have the right to prevent processing.

Direct Marketing

IFG will also follow the specific Direct Marketing guidance from the ICO to ensure we are marketing responsibly and ensure we are complying with the law. It covers the following steps:

Step 1: Identify - Does what you want to do count as direct marketing? Remember, direct marketing covers promoting aims and ideals as well as selling products and services.

Step 2: Plan - Take a data protection by design approach, planning how you will protect people's information from the start. Think about what information you want to use and how you want to get your direct marketing to people. And make sure you have a data protection reason ("lawful basis") for your direct marketing.

Step 3: Collect - Collect information for direct marketing fairly and clearly explain to people how you plan to use their information.

Step 4: Respect - Always respect people's preferences. People have an absolute right to object to or opt out of direct marketing at any time.

Roles and Responsibilities

The role responsible for IFG's data protection is the Data Protection Lead and this is the Marketing & Partnerships Director.

This person will be responsible for ensuring IFG keeps up to date with GDPR and associated legislation, will be the primary point of contact for the ICO and will ensure all staff are appropriately trained.

Training

New employees must read and understand this policy as part of their induction. All employees receive training covering basic information about confidentiality, data protection and the actions to take upon identifying a potential data breach. All employees are trained to protect individuals' data to which they have access, to ensure data security and to understand the consequences to themselves and IFG of any potential breaches of the provisions of this policy.

Contacting Us

If you have any questions about this Data Management and Protection Policy or other matters that relate to it, you may contact us, via our normal email or telephone numbers listed on our website.

Complaints

Internal complaints

If you have any concerns about our use of your personal information, you can make a complaint to IFG's Data Protection Lead: s.green@intfoundationgroup.co.uk

External complaints

If you are unhappy with how we have used your data, you can complain to the Information Commissioner's Office (ICO) by writing to:

Information Commissioner's Office
Wycliffe House
Water Lane

Wilmslow
Cheshire SK9 5AF

Helpline number: 0303 123 1113
ICO Website: https://www.ico.org.uk

Useful Links

Information Commissioner's Office: https://ico.org.uk/

Data Protection Act https://www.gov.uk/data-protection