Data Protection Policy

1. Overview

The Institute for Fiscal Studies (IFS) is a research organisation which processes information as an essential part of its business function. We process personal information to enable us to undertake research on a range of topics including (but not restricted to) economics, education and health, to maintain our accounts and records and to support and manage our staff.

IFS will comply with all legislative and regulatory requirements and this policy will be monitored and updated as required.

The information in this policy applies to the entire workforce at the IFS. Non-compliance may result in disciplinary action.

Zoe Oldfield (Head of Data Services) is responsible for implementation and operation of this policy. Zoe Oldfield (zoe_o@ifs.org.uk) is main point of contact for the policy and for any queries relating to the processing of personal data. Yani Tyskerud (yani_t@ifs.org.uk) or Emma Hyman (Emma_h@ifs.org.uk) are the secondary points of contact.

2. Registration

The IFS is registered with the Information Commissioner's Office as a controller under registration number Z5758698. The Data Protection Officer is Zoe Oldfield (Head of Data Services).

3. Privacy Policy

A privacy policy is published on the IFS website and can be found here:
https://www.ifs.org.uk/privacy

Staff privacy notice is available here: P:\Policies\Data protection, security and ICT\GDPR\Privacy Policies\Employee privacy notice.docx.

4. Legal Obligations

As a controller of personal data IFS is obliged to comply with data protection legislation in force in the UK (including the UK GDPR, the Data Protection Act 2018 (DPA) and the Privacy and Electronic Communications Regulations 2003 (PERC) (Data Protection Legislation). In our processing of personal data, we need to abide by the data protection principles embodied in Data Protection Legislation, which require that personal data shall be:

(a) processed lawfully, fairly and in a transparent manner in relation to individuals **('lawfulness, fairness and transparency');**

(b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in

the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes **('purpose limitation');**

(c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed **('data minimisation')**;

(d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay **('accuracy');**

(e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals **('storage limitation'**);

(f) 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 **('integrity and confidentiality'**).

The following steps need to be followed when working with personal data:

https://intranet.ifs.org.uk/share/page/site/ifs-net/wiki-page?title=Necessary_steps_for_IFS_researchers

4.1 How these obligations are met

IFS meets the legal obligations contained in the Data Protection Legislation in the following ways:

Lawfulness, fairness and transparency

IFS will only process personal data where we have valid legal basis. IFS will maintain a register of data processing activities and keep this up to date. This will document the legal basis under which the data are processed. Separate registers are kept for research data, human resources data and recruitment data. Where the IFS collects personal data from research participants, direct privacy notices will be issued to data subjects and these will be written in a clear, concise way, giving the data subject (research participant) all the necessary information in a transparent manner. Each new large-scale research data collection activity will be registered with the IFS or UCL data protection office and obtain a registration number. A detailed set of steps that must be taken when IFS collects data from research participants can be found here.

Where the IFS uses secondary data that is in scope of the UK GDPR (or the EU GDPR) but where it is not possible to issue individuals with a direct privacy notice, information for data subjects will be added to the IFS privacy page https://www.ifs.org.uk/privacy. Details of how an individual can find out what information that the IFS holds about them is also given on the privacy page.

Where the processing is likely to result in high risks to data subjects' rights and freedoms, before starting the processing we will need to carry out and document a data protection impact assessment.

Purpose Limitation

IFS will only ever process data for the purposes specified in the privacy notice. In addition to complying with privacy notices, for research data, this principle is a key part of data sharing agreements that IFS is party to.

Data minimisation

The IFS will ensure that any personal data are adequate, relevant and necessary in relation to the purpose for which they are processed. This principle is a key part of data collection and data sharing agreements that IFS is party to i.e. we collect, process and share only the minimum amount of personal data required for the purpose. Third parties from whom we receive personal data also do not permit the IFS to use data that is not necessary for the requested purpose.

Accuracy

The IFS will take reasonable steps to ensure personal data is accurate. Where we use secondary data, that has been pseudonomised (and therefore it is not easy to identify a data subject), we will inform the data owner if we become aware that there are inaccuracies in the data.

Storage limitation

The IFS has an appropriate data retention policy in place for all types of data that it processes. This can be found here: "P:\Policies\Data protection, security and ICT\GDPR\Data Retention\IFS Data Retention Policy.docx". This retention policies must be followed and data that reaches the end of the retention period must be securely deleted.

Integrity and confidentiality

The IFS will ensure that personal data are stored securely according to the policies that it has in place. These policies include those relating to ISO27001 compliance, Cyber Essentials and other specific arrangements contained in data sharing agreements that IFS is party to. IFS will implement and at all times maintain technical and organisational measures appropriate to the risks involved.

Zoe Oldfield and Emma Hyman share the role of Information Security Manager as part of the Information Security Management System. Andrew Reynolds is responsible for maintaining and implementation information security standards on the ICT system.

Accountability

The IFS must maintain records documenting various aspects of data processing (see 4.2 below). We may be required to make data protection records available to the Information Commissioner's Office (the ICO) on request. Documenting our processing activities is important, not only where it is a strict legal requirement under Data Protection Legislation but also in other cases as a matter of good practice, because it supports good data governance and can help the IFS demonstrate our compliance with Data Protection Legislation.

4.2 Documentation

Appropriate documentation relating to data protection will be kept up to date. This includes (but is not limited to): Legitimate Interest Assessments (where appropriate), Data Protection Impact Assessments (where necessary), records of consent (where necessary), Registers of Data

Processing Activities, Contracts with Data Processors, Data Sharing Agreements with other Data Controllers, data flows, records relating to data subjects' requests, retention records. Information is entered into the Register of Data Processing Activities.

4.3 Privacy Impact Assessment

The data protection registration form contains a privacy screening checklist. This guides applicants towards completing a Data Protection Impact Assessment when certain high-risk criteria are met OR to consider carrying out a DPIA

4.4 Special Categories of Data

Where Special Categories of data are used (as defined by Article 9 of the UK GDPR), both an Article 6 legal basis and an appropriate condition under Article 9 of the UK GDPR and/or the DPA 2018 for doing so will be recorded and documented.

4.5 Third party partners or vendors

The IFS may share personal data with external partners who will process personal data as independent controllers or joint controllers with the IFS. An appropriate contract needs to be entered into. Contracts and data sharing agreements must be approved and signed by Research Services.

We may need to disclose personal data to vendors whose services require the processing of personal data on the IFS's behalf and on the IFS's instructions. The IFS must enter a data processing agreement complying with the requirements of Article 28 of the UK GDPR. Data processing agreements must be approved and signed by Research Services.

4.6 Transfer outside of the UK

Where data is transferred outside of the UK, the IFS will need to comply with the restrictions in Chapter V of the UK GDPR. That means:

1) checking whether the data will be transferred to an adequate third country (i.e. a third country that the UK considers as providing an adequate level of protection for personal data); and

2) where personal data is to be transferred to a non-adequate third country, appropriate contracts will be used that include Standard Contractual Clauses valid in the UK and further requirements required to legitimise such transfers will be complied with on case-by case basis.

4.7 Individual rights

The following individual rights are respected in line with the law. Not all rights will be applicable to all circumstances. Direct privacy notices which state which rights are applicable will be issued where appropriate.

- The right to be informed
- The right of access
- The right to rectification
- The right to erasure
- The right to restrict processing
- The right to data portability
- The right to object to processing

- Rights in relation to automated decision making and profiling

Individuals wishing to exercise any of these rights on their own behalf or who have been asked to exercise any of these rights on behalf of a data subject should email dataprotectionofficer@ifs.org.uk

If you believe that the IFS has not complied with your data protection rights, you can complain to the Information Commissioner.

4.8 Data Subject Access Requests (DSARs)

Individuals can make a Data Subject Access Request by emailing: dataprotectionofficer@ifs.org.uk. Once a Data Subject Access Request is received, the Data Subject Access Request Policy will be followed. Head of ICT, the Head of Operations and the Head of Data Services will meet to discuss the SAR and how the request can best be met. The ICO Code of Practice for SARs will be followed.

All staff are given basic training on Subject Access Requests and how to escalate them. In addition, staff who have been identified as most likely to receive a request are given additional training.

5. Statistical Disclosure

The GSS Guidance on Statistical Disclosure Control must be followed: https://gss.civilservice.gov.uk/policy-store/anonymisation-and-data-confidentiality/

6. Data Protection Breaches

Where a Data Protection breach occurs the policy for notification of Personal Data Breaches will be followed.

7. Policy review and audit log

7.1 Summary of audit and review findings

Date	Reviewed by	Audited by	Issues found	NC or Obs?	Action taken	Location of audit findings*
21/6/21	EH	EH	None			
17/05/2022	ZO	ZO	No major issues found. Policy has been reviewed by a lawyer in the past year. Various links corrected.	obs	Links corrected	P:\Policies\Data protection, security and ICT\ISO27001\Policies and internal audits\7. Internal audit and review\Internal audits\2021_22

*all audit findings are stored in subfolders within ISO27001\Policies and internal audits\7. Internal audit and review\

7.2 Log of changes made

Date	Changes made	Changes made by	Approved by	Major or minor change?	Where archived?* (major changes only)
28/09/2021	Updated to reflect lawyer's comments	ZO	EH	major	Data Protection Policy\ Data

					Protection Policy 2021_09_28
17/05/2022	Link to the Staff Privacy Notice, the Data Subject Access Requests Policy and the Personal Data Breaches Policy corrected	ZO		minor	

*all archived documents are stored in subfolders within ISO27001\Working documents and archive\Archive