Data Subject Deletion Request Policy

1. Background

The UK General Data Protection Regulation (GDPR) allows individuals to request that their personal data are deleted. This is known as the "right to erasure" and is not absolute and only applies in certain circumstances. Guidance on when the right to erasure applies can be found here: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/individual-rights/individual-rights/right-to-erasure/. In particular, the right to erasure does not apply if the processing is necessary for archiving purposes in the public interest, scientific research, historical research or statistical purposes where erasure is likely to render impossible or seriously impair the achievement of that processing. Much of the work that the institute carries out falls under this criterion. Nevertheless, for ethical reasons, the option to request withdrawal from a study and deletion of data is often given regardless of any lack of legal obligation. This policy sets out the process for carrying out data deletion of individual data subjects. The Data Subject Access Request Policy should also be referred to:

- Subject Access Request Policy

2. Identifying a Data Subject Deletion Request

Deletion requests may be made

- Verbally,
- In writing
- Via social media
- To any part of the IFS (e.g to mailbox, to IT, to specific researchers)
- Via a third party organisation who may be collecting data on our behalf

Requests do not specifically have to mention any phrases from the UK GDPR. The Data Protection Officer should be notified of any data deletion request immediately.

3. Staff training

The IFS does not hold identifiable data about the general public. Data deletion requests are most likely to be received by the following categories of data subjects:

1. Members of staff or associates
2. Former members of staff or associates
3. Individuals on our mailing list
4. Individuals who have attended IFS events
5. Individuals who have taken part in surveys run by IFS where we hold personal data

For this reason, staff working in HR, communications, ICT and data services are made aware of this policy. In addition, research staff who are involved in collecting data are also given made aware of this policy and the process for handling data deletion requests.

Research staff are also made aware that if the receive a data deletion request in relation to de-identified data, they should suggest that the data subject gets in contact with the relevant organisation that collected the data.

4. Charging a fee

A fee will not be charged for data deletion.

5. IFS Procedures: Responding to Data Subject Deletion Requests

Action		**Time frame from time request received**
When a request is received, the Data Protection Officer (dataprotectionofficer@ifs.org.uk) should be notified immediately.	Staff member who receives the request	immediately
Consider whether the data should be deleted or whether an exemption applies. This decision should be made in line with data protection law and any privacy notices issued. Ethical considerations may also inform the decision.	DPO or researcher(for research data)	immediately
If the request comes from a data subject that is part of secondary data where we cannot identify the data subject, the data collector should be informed.	DPO	immediately
All Data Subject Deletion Requests will be logged on the Subject Access Request register with the date received. The Subject Access Request register is located here: P:\Policies\Data protection, security and ICT\GDPR\Subject Access Requests\SARS log.xlsx and is maintained by the Data Protection Officer. All requests logged on the SARs Register will be anonymised. The register logs the following details: ➢ Data request received ➢ Type of data subject ➢ Type of request ➢ Date of reply ➢ Outcome	DPO. In the absence of the DPO, responsibility lies with the Head of Operations	As soon as possible
In addition to the anonymised register, where data deletion relates to a data subject that is part of research study, researchers may wish to keep their own log. This may only contain identifiable information that is necessary for auditing purposes (provided that information is stored securely). Any identifiable information should be deleted within three months.	Researcher	As soon as possible
If you are not sure the requester is who they say they are you should check this by asking questions that only the individual would know. For example, if it is an ex-employee, ask who their line manager was and the dates that they worked for IFS.	DPO	As soon as possible
In the case of non-research data, alert key IFS individuals regarding the receipt of the request and timeline. This may include: • Head of Operations • Head of ICT • Director; • Head of Finance; • Senior members of the Computing Committee and; as necessary	DPO	As soon as possible

• Line Manager and Sector Head (employee request) • Head of PR and Head of Communications (external request)		
Agree (through convening meetings or email correspondence) an owner for the data subject deletion request, responsible for working with others to prepare the response.	DPO with key IFS individuals	
With key IFS individuals, brainstorm all sources of relevant information. This may include (but is not limited to): - Email including the jobs@ifs.org.uk inbox - Network files - Hard copies of HR information - Marketing databases - Events databases - Research data collection - Recruitment	DPO with key IFS individuals	
Assign responsibility to searching depending on where the information will be found. E.g historical email will be searched by IT, marketing or events databases will be searched by comms, research data collections will be searched by the relevant member of res	Key individuals	2 weeks
Gather together all the relevant information and delete it.	DPO with key IFS individuals	3 weeks
Prepare your reply. Consult the templates contained in section 6 of this policy. In the case of research data where requests were received by a third-party collecting data on our behalf, ensure that the third party sends the reply on our behalf but request confirmation from the third party that this has been done.	DPO (non research data) Researcher (research data)	Less than one calendar month
Keep a record of the reply in the SARs log (and any other logs being kept)	DPO	One calendar month

6. IFS Template letters for responding to Subject Access Requests

Four templates are included on the following pages:

- Letter confirming data deletion request.
- Letter rejecting data deletion request
-

Letter confirming deletion

Dear [ ]

Thank you for [submitting your form/your email] on [date], making a request for your personal data to be deleted.

Following your request, we would like to confirm that your personal data has been effectively and completely deleted from our systems. [All of our service providers were directed to do so as well. Each has confirmed that your data has been erased.]

[You will not be contacted again].

We trust that this responds sufficiently to your request.

Yours sincerely

[ ]

Letter rejecting deletion

Dear []

Thank you for [submitting your form/your email] on [date], making a request for your personal data to be deleted.

Unfortunately, we cannot process your request at this time.

The reason for this is: (please delete as appropriate. These are the most likely reasons but there may be others)

[The data we hold does not contain enough information for us to identify you. In our research, we use data that has been anonymised. If you would like your information to be deleted, you should contact [X] which is the organistion that collects the data and holds your personal information]

[We are unable to find any records associated with you on our systems]

[The processing of your data is necessary for archiving purposes in the public interest, scientific research, historical research or statistical purposes and erasure is likely to render impossible or seriously impair the achievement of that processing. Under UK law, this means that your right to erasure does not apply]

[The right to erase conflicts with other legal statutory or contractual record retention periods, such as, financial laws and regulations that require us to maintain your information for a period of time.]

We trust that this responds sufficiently to your request.

Yours sincerely

[ ]

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*

*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)

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