# Data Protection Policy

## Introduction:

The Faraday Institute for Science and Religion (FI) is committed to protecting the rights and privacy of individuals in accordance with the UK GDPR (General Data Protection Regulation).

This policy applies to all staff of FI, except when they are acting in a private or external capacity. For clarity, the term staff means anyone working in any context for FI at any level or grade (whether permanent, fixed term or temporary) and including employees, retired but active members and staff, workers, trainees, consultants, seconded staff, agency staff, agents, volunteers, and external members of Institute committees, including Trustees.

## Legal Definition of personal information

Personal information is defined as data or other information about a living person who may be identified from it or combined with other data or information held. Some "special category data" (formerly sensitive personal data) are defined as information regarding an individual's racial or ethnic origin; political opinion; religious or other beliefs; trade union membership; physical or mental health or condition; sexual life; or criminal proceedings or convictions, as well as their genetic or biometric information.

An individual's rights (all of which are qualified in different ways) are as follows:

- The right to be informed of how their personal data are being used. This right is usually fulfilled by the provision of 'privacy notices' (also known as 'data protection statements' or, especially in the context of websites, 'privacy policies') which set out how an organisation plans to use an individual's personal data, who it will be shared with, ways to complain, and so on;
- The right of access to their personal data;
- The right to have their inaccurate personal data rectified;
- The right to have their personal data erased (right to be forgotten);
- The right to restrict the processing of their personal data pending its verification or correction;
- The right to receive copies of their personal data in a machine-readable and commonly-used format (right to data portability);
- The right to object: to processing (including profiling) of their data that proceeds under particular legal bases; to direct marketing; and to processing of their data for research purposes where that research is not in the public interest;
- The right not to be subject to a decision based solely on automated decision-making using their personal data.
- The right to know what personal data is held about them.

## Data Protection Principles

Data protection law applies to the processing (collection, storage, use and transfer) of personal information (data and other personal identifiers) about data subjects (living identifiable individuals).

Personal data must:

1. Be processed fairly and lawfully and only when certain conditions are met.
2. Only be obtained and processed for specified and lawful purposes.

3. Be adequate, relevant and not excessive.
4. Be accurate and, where necessary, up to date.
5. Be kept for no longer than necessary.
6. Be processed in accordance with data subjects' rights.
7. Be protected by appropriate security measures.
8. Not be transferred outside the UK to countries without adequate protection unless explicit consent of the data subject has been obtained.

The Regulation defines both personal data and special personal data (for definitions, please see Appendix 1). Data users must ensure that the necessary conditions are satisfied for the processing of personal data. In addition, they must adhere to the extra, more stringent conditions in place for the processing of special personal data. Special personal data should normally only be processed if the data subjects have given their explicit (written) consent to this processing, and must be protected with a higher level of security. It is recommended that special records are kept separately in a locked drawer or filing cabinet, or in a password-protected computer file. (We note that information about religious beliefs is special data.)

## Security

The security of personal data in the possession of FI is of paramount importance and is therefore addressed in various policies and procedures. The FI security procedures include:

- Entry controls to prevent unauthorised people gaining access to confidential information and personal data.
- Lockable desks and cupboards for secure storage of confidential information and personal data.
- Shredding for paper records with confidential information and personal data that is no longer being stored.
- Ensuring unauthorised people are not able to see confidential information on paperwork or computer screens being used by staff.

## Use of personal data

Use of personal data must be only in accordance with FI Data Protection Policy and Privacy notices. If other uses are required, the relevant privacy notice must first be updated and the data subjects covered by the notice informed.

## Responsibilities – General Principles

All personal data held on behalf of the FI, whether electronically or on paper, must be kept securely, no matter whether it is kept by an individual or on the commonly-accessible server. Personal data must not be disclosed to any unauthorised third party by any means. Where staff are unsure as to whether they can legitimately share/disclose personal data with other individuals, either within or outside the FI, they must seek advice from their line manager. All staff should note that unauthorised disclosure may be a disciplinary matter. It may also be a criminal matter for which the FI and the individual concerned could be held criminally liable

## Data Protection Officer Responsibilities

FI shall appoint a statutory Data Protection Officer, who will be responsible for:

- All staff are aware of their responsibilities under the Data Protection Policy and the Regulations and of the risks/consequences of failure to comply with the related requirements.

- That mechanisms are put in place to protect data (and particularly special data) during day to- day operations.
- All personal data being processed within the FI complies with the Regulations.
- That all forms and correspondence used by the FI to request personal data clearly state the purposes for which the information is to be used, the period of time it is to retained, and to whom it is likely to be disclosed.
- All personal data held within the FI is kept securely and is disposed of in a safe and secure manner when no longer needed.
- All Data Protection breaches are notified to the Data Protection Officer, with remedial action taken to mitigate the risk of reoccurrence. Record and report upon any breaches.
- An annual audit of the personal data within the FI is carried out and recorded.
- Where a new or different purpose for processing data is introduced, the policy and/or privacy notices are updated.
- The FI's Data Protection Policy is regularly reviewed by the Trustees and updated in line with best practice.
- Staff have access to training on their responsibilities under the Data Protection Policy and the Regulation, both on-line and through more traditional training methods.
- Responses to requests for information under the Regulation, and related compliance matters, are dealt with in a timely manner and in line with the requirements of the Regulation.
- Advice and guidance on any area of the Policy or the Regulation is provided to staff and students, on request.

## Staff Responsibilities

All staff must take personal responsibility for ensuring that:

- They are aware of their responsibilities under the Data Protection Policy and the Regulation and the risks/consequences of failure to comply with the related requirements. Where they are uncertain of their responsibilities, they must raise this with their manager.
- They complete on-line training if they require further information about data security.
- Personal data relating to any living individual (staff, trustees, students, contractors, members of the public etc.) which they hold or process is kept securely.
- Personal data relating to any living individual is not disclosed, either orally or in writing, accidentally or otherwise, to any unauthorised third party.
- All Data Protection breaches are notified to their manager, with remedial actions implemented to mitigate the risk of reoccurrence.
- When supervising those not employed by FI who are processing personal data, that they are aware of this policy.
- Personal data which they provide in connection with their employment is accurate and up-to date, and that they inform FI of any errors, corrections or changes, for example, change of address.
- Passers-by cannot read confidential information from papers or computer monitors; this includes locking computers when left unattended.
- Never giving out personal information by telephone without being confident that the caller is entitled to it; requests by email should be encouraged.

## Retention Policy for Personal Data Records

The Regulation places an obligation on the FI not to hold personal data for longer than is necessary. The FI's policy on retention of records is held in a separate policy.

## Transfer of Data Outside the Faraday Institute

When FI shares personal data with another organisation, liability for adherence to the Regulation, in relation to this data, rests with the FI. Should the receiving organisation breach the Regulation, FI would be held responsible for that breach. A data sharing agreement may be required before sharing personal data with other organisations in order to conduct business.

## Transfer of Data Overseas

The Eighth Data Protection Principle prohibits the transfer of personal data to any country outside the UK unless that country ensures an adequate level of protection for data subjects. In all instances where personal data is being sent outside the UK, the consent of the data subject should be obtained before their personal information is sent. This includes requests for personal data including from overseas colleges, financial sponsors and foreign governments.

## GDPR for Researchers

(a) Researchers will identify the appropriate legal basis for data processing for their project. In almost all cases, the recommended legal basis for normal personal data is that the data processing is necessary for the performance of a task carried out in the public interest, and the recommended legal basis for special category (sensitive) personal data is that the processing is necessary for scientific or historical research purposes in the public interest. The recommended legal basis for data processing is **not** consent (or explicit consent), even when consent is collected from research participants for ethical reasons.

(b) Researchers will have adequate data management plans/arrangements in order to meet the other data handling and security principles in *the GDPR General Principles*.

(c) Researchers will ensure that the information they supply to research participants about how their personal data will be used in the project covers all the topics required in order to fulfil the right in *the UK GDPR General Principles*. There is a partial exemption from the supply of this personal if the data has not been collected from the data subjects themselves, and if to supply the information would be impossible or would involve disproportionate effort (e.g. you have no or very limited contact details). In such circumstances you should endeavour to make the relevant information publicly available (e.g. on a website).

(d) Ethical reviews for high risk research projects will continue to be required.

## Privacy notices

The privacy notice provided on the website should be read in conjunction with this policy.

## Use of images

FI will gain the consent of individuals whose images are used for marketing and PR activities, including in print, online and on social media. We acknowledge that restrictions can be put on staff using such images in their personal publishing but that other people are outside the Trust's control.

## Making a Request

Staff, students, users of the FI's facilities, and members of the public have the right to access personal data that is being kept about them insofar as it falls within the scope of the Regulation. Requests should be made in writing via email to admin@faraday.cam.ac.uk or by post to The Faraday Institute for Science and Religion, The Woolf Building, Madingley Road, Cambridge CB3 0UB. The FI does not

charge an administrative fee to access information and will seek to ensure that the information is provided within 30 calendar days. There is no right to an internal review of a decision taken regarding release of personal information. If the requestor is not satisfied with the response received from the FI they do, however, have the right to appeal directly to the e Information Commissioner's Office at Wycliffe House, Water Lane, Wilmslow, SK9 5AF (ico.org.uk).

## Accountability

The Institute is required under law to:

• comply with data protection law and hold records demonstrating this;
• implement policies, procedures, processes and training to promote "data protection by design and by default";
• have appropriate contracts in place when outsourcing functions that involve the processing of personal data;
• maintain records of the data processing;
• record and report personal data breaches;
• carry out, where relevant, data protection impact assessment on high risk processing activities;
• cooperate with the Information Commissioner's Office (ICO) as the UK regulator of data protection law;
• respond to regulatory/court action and pay administrative levies and fines issued by the ICO.

### Data Breaches

- A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes.A data breach must be reported to admin@faraday.cam.ac.uk and the Director as soon as the employee realises the breach has occurred.
- The data breach log to be completed by Administrator.
- Decision to be taken by the Director as to whether breach is sufficiently serious to be referred to the Trustees.
- Trustees have the responsibility for deciding whether the incident should be reported to the ICO. The ICO must be notified within 72 hours of the Institute becoming aware of the breach.
- If the breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms, those individuals must be made aware of the breach without undue delay.
- In cases where the breach has not been reported to the ICO, a serious incident may still need to be reported to the Charity Commission.

The Faraday Institute for Science and Religion

## APPENDIX 1

## Definitions

**Data** - Information which is being used or held in a computerised system, or a 'relevant filing system' i.e. a manual filing system that is structured in such a way that data contained within it is readily accessible. Data can be written information, photographs, fingerprints or voice recordings.

**Personal Data** - Information that identifies and relates to a living individual, and includes any expression of opinion or intention about the individual.

**Special Personal Data** - Personal data consisting of information as to race/ethnic origin; political opinion; religious or similar beliefs; trade union membership; physical or mental health or condition; sexual life; and criminal record.

**Data Controller -** The data controller determines the purposes for which and the means by which personal data is processed.

**Data Processing** - Anything which can be done with personal data i.e. obtaining, recording, holding, organising, adapting, altering, retrieving, consulting, disclosing, aligning, combining, blocking, erasing, destroying etc.

**Data Subject** - An individual who is the subject of personal data. This will include: staff, current and prospective students, graduates, suppliers of goods and services, business associates, conference delegates, survey respondents etc.