Data Protection Policy, including Key Procedures

Foundation for Liver Research (Institute of Hepatology)

HEADING	SECTION CONTENT
Aims of this Policy	The Foundation for Liver Research (Institute of Hepatology) (hereafter "FLR") needs to keep certain information on its employees, trustees and donors to carry out its day to day operations, to meet its objectives and to comply with legal obligations. The organisation is committed to ensuring any personal data will be dealt with in line with The General Data Protection Regulation (GDPR), a new EU law that will come into effect on 25 May 2018 to replace the Data Protection Act 1998. To comply with the law, personal information will be collected and used fairly, stored safely and not disclosed to any other person unlawfully. The aim of this policy is to ensure that everyone handling personal data is fully aware of the requirements and acts in accordance with data protection procedures. This document also highlights key data protection procedures within the organisation. This policy covers employed staff, trustees and other representatives of the FLR.
Definitions	The FLR will ensure that it adheres to the core principles of the GDPR Article 5 of the GDPR requires that personal data shall be: a) processed lawfully, fairly and in a transparent manner in relation to individuals; 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; c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

	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; 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; and 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." Article 5(2) requires that: "the controller shall be responsible for, and be able to demonstrate, compliance with the principles" The definition of 'Processing' is obtaining, using, holding, amending, disclosing, destroying and deleting personal data. This includes some paper based personal data as well as that kept on computer.
Type of information processed	The FLR processes the following personal information: • Information on applicants for posts, including references • Employee information – contact details, bank account number, payroll information, supervision and appraisal notes. • Trustee information - contact details • Donor information - contact details Personal information is kept in the following forms: paper based and computer based systems. Groups of people within the organisation who will process personal information are: employees and in the case of payroll, the Charity Payroll Service
Notification to the Information Commissioner	The needs we have for processing personal data are recorded on the public register maintained by the Information Commissioner. We notify and renew our notification on an annual basis as the law requires. If there are any interim changes, these will be notified to the Information Commissioner within 28 days. The name of the Data Controller within our organisation as specified in our notification to the Information Commissioner is Natalie Day
Responsibilities	Overall responsibility for personal data in a voluntary organisation rests with the governing body. In the case of the FLR, this is the Board of Trustees.

	The governing body delegates tasks to the Data Controller. The Data Controller is responsible for: • understanding and communicating obligations under the GDPR • identifying potential problem areas or risks • producing clear and effective procedures • notifying and annually renewing notification to the Information Commissioner, plus notifying of any relevant interim changes All employed staff who process personal information must ensure they not only understand but also act in line with this policy and the data protection principles. Breach of this policy will result in will result in disciplinary proceedings
Policy Implementation	To meet our responsibilities, staff and trustees will: • Ensure any personal data is collected in a fair and lawful way; • Explain why it is needed at the start; • Ensure that only the minimum amount of information needed is collected and used; • Ensure the information used is up to date and accurate; • Review the length of time information is held; • Ensure it is kept safely; • Ensure the rights people have in relation to their personal data can be exercised We will ensure that: • Everyone managing and handling personal information is trained to do so. • Anyone wanting to make enquiries about handling personal information, whether a member of staff, Trustee or donor, knows what to do • Any disclosure of personal data will be in line with our procedures. • Queries about handling personal information will be dealt with swiftly and politely
Training	Training and awareness raising about the GDPR and how it is followed in this organisation will take the following forms: On joining the IoH: ▪ Staff will be given a copy of the Data Protection Policy ▪ Staff will be given a copy of the Employee Handbook General training/ awareness raising: The importance of Data Protection and requirements of the GDPR will be discussed as part of the annual appraisal, both in relation to personal data of staff and also any data for which they might be responsible as part of their duties.

Gathering and checking information	Before personal information is collected, we will consider: • What details are necessary for specific purposes • How long we are likely to need this information We will inform people whose information is gathered about the following: • why the information is being gathered • what the information will be used for • who will have access to their information (including third parties) We will take the following measures to ensure that personal information kept is accurate: • An annual request to staff to confirm their details as part of the appraisal process • A request to Trustees to confirm their details, made in conjunction with the audit requirements of the FLR's annual report and accounts • The FLR's periodic newsletter includes a request to recipients to confirm their willingness for the FLR to retain their details for the specific purpose of keeping recipients of the newsletter up to date with the work of the FLR. Personal sensitive information (PSI) will not be used apart from the exact purpose for which permission was given. PSI is information about ethnic origin, political opinions, religious beliefs, membership of a trade union, physical or mental health, criminal convictions etc. Consent must be sought each time it is to be used. This information will only be captured for a specific purpose e.g. to explain absence. In the event the FLR wishes to use the information for another purpose, even a related purpose, we will seek specific consent to do so.
Retention periods	FLR will ensure that information is kept according to the following retention periods guidelines • Personnel files - 6 years after employment (slimmed down format after 2 years) • Application forms and interview notes (unsuccessful candidates) - 1 year • Letters of reference - 6 years from the end of employment • Redundancy details - 6 years from the date of redundancy • Parental leave - 5 years from birth/adoption or 18 if child receives a disability allowance • Accident books, accident records/reports - 3 years • Assessments under health & safety regulations - permanently • Income tax, NI returns, income tax records and correspondence with IR - at least 3 years after the end of the financial year to which they relate • Statutory maternity pay records and calculations - at least 3 years after the end of the financial year to which they relate • Statutory sick pay records and calculations - at least 3 years after the end of the financial year to which they relate • Wages and salary records - 6 years • Employee joining/new starter form - 6 years after employment ceases

Data Security	The organisation will take steps to ensure that personal data is kept secure at all times against unauthorised or unlawful loss or disclosure. The following measures will be taken: • Use of lockable cupboards and filing cabinets (restricted access to keys) • Password protection on personal information files • Setting up computer systems to allow restricted access to certain areas • Not allowing personal data to be taken off site (as hard copy, on laptop or on memory stick) • Back up of data on computers (onto a server/the cloud off site) Any unauthorised disclosure of personal data to a third party by an employee may result in result in disciplinary proceedings Any trustee making an unauthorised disclosure of personal data to a third party could be personally liable for any penalty arising from a breach that they have made.
Procedure in case of a breach	When a breach of data protection occurs, consideration will be given to reviewing practices. In addition, the FLR will consider whether the breach should be reported to the Information Commissioner and/or to any partners with which we hold Information Sharing or Partnership Agreements. In addition to notifying the Information Commissioner, the FLR will also inform the following partners, as relevant, should any breach of data occur: donors, trustees, research collaborators, grant giving bodies
Subject Access Requests	Anyone whose personal information we process has the right to know: • What information we hold and process on them • How to gain access to this information • How to keep it up to date • What we are doing to comply with the GDPR They also have the right to prevent processing of their personal data in some circumstances and the right to correct, rectify, block or erase information regarded as wrong. Individuals have a right to access certain personal data being kept about them on computer and certain files. Any person wishing to exercise this right should apply in writing to Natalie Day, Head of Administration, Institute of Hepatology, 111 Coldharbour Lane, London SE5 9NT The following information will be required before access is granted: • Full name and contact details of the person making the request • Their relationship with the organisation (former/ current member of staff, trustee or other service user) • Any other relevant information e.g. timescales involved We may also require proof of identity before access is granted (e.g. passport, birth certificate etc)

	Queries about handling personal information will be dealt with swiftly and politely. We will aim to comply with requests for access to personal information as soon as possible, but will ensure it is provided within the 40 days required by the Act from receiving the written request.
Review	The FLR's Data Protection Policy and measures to ensure organisational compliance are included in the FLR's Risk Register and as such will be reviewed on an annual basis by the trustees.