



The London Irish Centre [LIC] Data Protection Policy

Contents

1. Purpose and Scope
2. Principles
3. Data Definitions
4. Data Held and Processing of Data
5. Recruitment Data Collected from Applications
6. Employee Monitoring
7. Security
8. Unauthorised Disclosure
9. Individual Access Rights
10. Exemptions from Disclosure

1. Purpose and Scope

- 1.1 To explain the rules for processing personal information and the types of information The LIC will typically hold, and to ensure individuals are aware of their rights concerning the use of personal data which may be held on them. This will include personal information which is provided during the recruitment process, and will therefore also ensure applicants are aware of their rights concerning the use of personal data which may be held on them.
- 1.2 The policy covers all employees on the payroll; former employees; agency workers; internal and external applicants for employment within The LIC; including transfers within the organisation; volunteers and Board members. There is a separate The LIC policy in relation to client data. This policy is only concerned with data generated in relation to potential employees, employees and former employees.

2. Principles

- 2.1 An individual has a right to expect that personal and sensitive personal information disclosed by them to designated staff and or managers, or which is generated by The LIC in the course of their employment or potential employment, will be protected by The LIC is fairly and lawfully obtained and processed in accordance with legitimate business and legal requirements, securely held and not shared with third parties without the individual's consent.
- 2.2 The LIC will comply with the Data Protection Act. The Act covers some manual records, such as those recorded on paper, as well as computerised records and is concerned with the processing of 'personal data', that is, data relating to identifiable living individuals.
- 2.3 The 'Data Controller' is The LIC Data will be processed by appointed representatives within the organisation, including managers and any individuals with specific responsibility for data processing. Agents (recruitment agencies, response agencies and photocopying companies) acting on behalf of The LIC in the recruitment process may also be data controllers. The Data Officer is the person who is responsible in the organisation for ensuring that The LIC complies with the Data Protection Act; this is currently the Operations Manager for data concerned with employment.
- 2.4 There are eight data protection principles that are central to the Act. In brief, they say that personal data must be:
 - Processed fairly and lawfully
 - Processed for limited purposes and not in any manner incompatible with those purposes adequate, relevant and not excessive
 - Accurate
 - Not kept for longer than is necessary
 - Processed in line with data subjects' rights
 - Secure
 - Not transferred to countries that don't protect personal data adequately.
- 2.5 The LIC recruitment processes are maintained to ensure they meet the Data Protection Act and are designed to ensure that applicants:
 - Are treated in a fair, timely and efficient manner;
 - Are only considered for the vacancy or vacancies they have applied for, or consent is sought before considering them for other vacancies inside or outside the organisation;
 - Understand the rationale used in assessing applications.
- 2.6 This Policy covers the Data Protection principles and an individual's rights as set down in the Data Protection Act. This policy does not form part of any individual employee's contract of employment with the LIC However it is the responsibility of every employee to familiarise

themselves with, and to comply with, this policy. Employees should ensure that they are referring to the current version, which is available on the Intranet.

3. Data Definitions

3.1 *Personal Data*

Personal Data is that which relates to a living individual who can be identified from the data or from a combination of that data with other information in the possession, or likely to come into the possession, of the holder. Data does not have to be private or sensitive in order to constitute personal data and includes information such as names, addresses, telephone numbers and information contained in a job application or CV, interview notes and references. Personal data covers both facts and opinions that are held about an individual. It also includes information regarding The LIC intentions towards the individual. Data relates to any information held on a computer (including e-mails) or manually held paper records that have been stored in a structured way so that information can be found easily or manual records which are due to be stored. This includes any records held by HR, managers or recruitment panel members.

3.2 *Sensitive Personal Data*

Sensitive personal data is defined as information about an individual's:

- Racial or ethnic origin;
- Political opinions;
- Religious beliefs or other beliefs of a similar nature;
- Trade union membership or non-membership;
- Physical or mental health or condition;
- Sex life;
- Criminal or alleged criminal offences or any proceedings for an offence or alleged offence.

4. Data Held and Processing of Data

4.1 *Examples of Personal Data which is likely to be held by The LIC*

Personal data which may be held by the The LIC includes the following:

- HR Personal Files and information stored on Cascade
- List of names and addresses whether on spreadsheet, paper or card indexes
- List of names, telephone numbers and or email addresses held by managers
- Paper based employee files containing employment records held by SMT (Contracts, Appraisals, Letters of communication etc.)
- References provided to, or received from, external sources (see References Procedure)
- Training Records, including personal development plans
- Support and Supervision records held by line managers
- Payroll and Pension records held by Finance.
- Information contained on e-mail which mentions the individual's name and of which they are the specific focus
- Computerised files holding information focusing on a specific individual
- Health records submitted to The LIC with the permission of the individual which may include medical certificates, medical appointment letters and Occupational Health reports.

4.2 This list is not exhaustive and will be subject to change.

4.3 *Purposes for which an employee's personal data will be processed*

The LIC will hold and process personal data provided by an employee for all purposes related to their employment including, but not limited to:

- Administering and maintaining personnel records;
- Paying and reviewing salary and other remuneration and benefits;

- Providing and administering benefits (including pension, life assurance and permanent health insurance);
- Undertaking performance appraisals and reviews, including talent review and succession planning;
- During performance, absence, disciplinary, harassment and bullying, grievance and redundancy proceedings;
- Providing references and information to future employers, and, if necessary, governmental and quasi-governmental bodies for social security and other purposes, the Inland Revenue and the DWP;
- Providing information to funders or potential funders
- Providing information to potential merger partners with The LIC.

4.4 *Purposes for which an employee's sensitive personal data will be processed*

Sensitive personal data will be processed as follows:

- [HR] will process racial or ethnic origin, sex, sexuality, age and disability for statistical monitoring purposes, in accordance with the Commission on Racial Equality and Disability Discrimination Act guidelines. This data will be used to measure The LIC's diversity profile in line with our diversity strategy.
- [HR] will process data on an employee's health for the purposes of maintaining sickness or other absence records, and taking decisions as to an employee's fitness for work and entitlement to related benefits (e.g. SSP and occupational sick. Details of work related injuries or illnesses will also be provided to the Health and Safety TU rep where requested and will be reported in accordance with The LIC's legal requirements.
- Payroll will process Trade Union membership details for the purposes of making deductions from salary for union subscriptions.
- a Senior Managers will process information on criminal offences (spent and unspent) in order to determine suitability for employment or continued employment, where appropriate.

4.5 Sensitive personal data may also be processed, in accordance with data protection legislation, to exercise or perform a right or obligation conferred or imposed by law on The LIC in connection with employment; in connection with legal proceedings or for the purpose of obtaining legal advice; or for administration of justice.

4.6 *Sharing of Information*

Information and the sharing of information is critical to the running of The LIC. Employees and third parties with whom The LIC has a business relationship, including arrangements which directly benefit employees, rely on fast, reliable access to information. For this reason, personal data is shared with and may be obtained from:

- Payroll Bureau
- Pensions Advisor and Pension Organisations and Trustees
- Occupational Health
- Statutory Authorities
- Government Agencies
- Funders
- Police
- Legal Advisors
- TU Officials
- Insurance Advisors and companies

4.7 This list is not exhaustive and will be subject to change.

4.8 An employee, who requires access to personal data held by a third party provider, should contact the provider directly.

4.9 *General guidelines for processing data*

Individuals who process personal data must comply with the following:

- Where specific personal information is sought from an individual, the individual should be informed as to the purposes for which that data will be processed
- Personal data obtained for a specified purpose should not be processed for another purpose without the individual's consent
- Any personal data processed should be adequate, relevant and not excessive in relation to the purpose for which it is held
- Personal data should be accurate and kept up to date. Managers will remind employees from time to time to check those of their personal details which are subject to change e.g. personal details such as home address.

4.10 *Retention of personal data*

Personal data should not be retained for longer than is necessary. Information should only be retained where there is a genuine organisational need to do so.

4.11 *Consent*

Employees are asked for their consent to keep and process sensitive personal data at the outset of their employment relationship.

5. Recruitment Data Collected from Applications

5.1 *Processing of Personal Data on Recruitment Applications*

All responses to advertisements, whether electronic or paper-based, will be submitted on the basis that the applicant consents to the processing of all their data, including sensitive personal data (see above). Applicants sign their consent on their application.

5.2 The LIC uses manual systems to consider applications against advertised positions using the relevant person specification and other similar vacancies where consent is given within The LIC.

5.3 The process for the receipt and distribution of applications is as follows:

- Applications are accepted via mail (e-mail and postal mail) for specific positions. For some positions, The LIC may request responses via external agencies.
- Speculative applications are also accepted via both types of mail but the applicant is either contacted to complete a full application where a suitable vacancy is available or the application is destroyed.
- Copying of applications may be carried out by The LIC or an agent acting on behalf of The LIC.
- Applicants are selected for positions based on skills, qualifications experience and competencies required by the job person specification.
- Applications are reviewed by recruitment panel members (managers and staff) and in some cases External recruitment consultants.
- Applications for a specific vacancy (including supplementary data produced by the process (e.g. marking sheet, interview notes, completed tests and results) will be retained by The LIC on paper, with basic details being entered into the HR recruitment database and on a test spreadsheet where applicable.
- If an application matches the criteria for another position (the criteria being that specified in the person specification), the applicant may be contacted to ascertain whether they are interested in the position and data will only be processed if consent is given.
- Applications may be electronically or manually shared between The LIC sites.
- Application data is reported on, in terms of volumes received from various sources of advert (e.g. newspaper, internet site, agency, recruitment fair, speculative etc.).

5.4 *Processing of Sensitive Personal Data for recruitment and subsequent employee monitoring*

Sensitive personal data is not used in the decision making process, except where the following circumstances are relevant to the position being considered:

- Details that the applicant has declared about any support, modifications, adjustments, or special equipment needed to assist them in carrying out the duties of the post taking into account The LIC's obligations under the Equality Act 2010; and
- Details of criminal offences spent and unspent convictions due to The LIC's Vulnerable Adult Client group.

5.5 The LIC will also process information on racial or ethnic origin, gender, sexuality, age and disability for statistical monitoring purposes only, in accordance with the Equality Act 2010 and other relevant guidelines.

6. Employee Monitoring

6.1 The LIC has the means, automated and otherwise, of monitoring individual usage of property and equipment including E-mail and the Internet. All traffic is automatically recorded to ensure that it is being used appropriately and The LIC may retrieve and read all this information at any time. In order to protect The LIC's charitable resources we reserve the right to use appropriate monitoring systems and information, and such information may form part of the evidence in any disciplinary or other management action that may be taken in connection with:

- Any breach of our rules relating to personal use of property, equipment and time
- Any other matter upon which individual usage of property, equipment and time has a bearing.

7. Security

7.1 The LIC will ensure that appropriate technical and organisational measures are taken to safeguard personal data. All databases containing personal data are password protected, and The LIC limits the number of people who will have access to the data.

7.2 Each individual has a personal responsibility to ensure that any information of a personal or sensitive personal nature to which they have access in the course of their work with The LIC is protected from unauthorised access and disclosure. This applies equally to data relating to employees and volunteers of The LIC, agency worker, Board members, consultants and contractors.

7.3 In particular, individuals must observe the following rules:

- Electronic storage of such material should be password protected
- Personal information sent to individuals should be labelled as 'Confidential – Addressee Only'
- Individuals must not disclose information about The LIC or any personal information about individuals other than in the course of proper performance of duties and or to authorised colleagues.
- Particular care must be taken when exchanging information with third parties to check that the person requesting information is who they claim to be and that there is proper authorisation or consent.
- Information must not be used for purposes other than that for which it was intended.
- All employees and managers to sign a confidentiality clause as part of their contract of employment with The LIC.
- In the event that an employee receives a request for information under the Data Protection Act this should be passed to [HR].

8. Unauthorised Disclosure

- 8.1 Individuals should be aware that disclosure of information in contravention of this Policy will be treated by The LIC as a serious disciplinary offence which may result in gross misconduct, and further that under the Data Protection Act individuals can be prosecuted for an improper use or unauthorised disclosure of such data.

9. Individual Access Rights

9.1 Informal Requests

An employee may make an informal request to view a particular file that their manager holds on them.

- 9.2 If the employee requests to see their Personal file held by the CEO it is important to ensure that the employee is only interested in viewing this file, rather than any other information held on them. If this is the case, a suitable time should be arranged for the employee to view their file with their manager and they may request copies of any documents contained within the paper based file or print out of pages from within the computerised file.

- 9.3 If the employee wishes to make a more comprehensive search thereby invoking the Act, the following Formal Request process should be followed. Current employees will not be charged to make a formal request but will need to put the request in writing as outlined below.

9.2 Formal Requests

Requests by an ex-employee, or other individual (e.g. an applicant) who has had any dealings with The LIC should always be considered as a formal request.

- 9.3 Under the Act, the employee, ex- employee or other individual is entitled:

- To be told whether anyone in The LIC is holding any of their personal data;
- If so, to be given a description of:
 - The personal data held;
 - The purposes for which the data is being processed; and
 - Those to whom the information is, has or may be disclosed.

- 9.4 If an individual want to make a formal request for access to any information held on them by The LIC:

- The individual should be advised to put a request in writing to CEO, enclosing the relevant fee of [£10] made payable to The LIC.
- On receipt of the fee the Operations Manager will check to ensure that the individual is who they claim to be, validate their right to gain access to the data and consider the appropriateness of the request in line with the Act.
- The Operations Manager will contact the appropriate individuals within The LIC and, where appropriate, any external organisations (e.g. referees), and request access to or copies of the relevant information held on that individual within any system or manual file (e.g. printouts of computer held records, copies of paper-based records).
- The information, once collated, should be made available within 40 days from receipt of the fee, unless the burden of providing the information is excessive.

- 9.5 In some circumstances it may be appropriate for the Operations Manager and a member of SMT to agree an appropriate time for the individual to review the information held on file, and take copies of documents, as appropriate. Where appropriate, any inaccuracies identified by the requesting individual will subsequently be amended.

10. Exemptions from Disclosure

- 10.1 In line with the Data Protection Act The LIC will not disclose information in the following circumstances:

- Confidential references provided by The LIC for current or ex-employees.
- References supplied to The LIC, unless the provider has consented or disclosure is otherwise reasonable in the circumstances.
- Personal data processed for the purposes of management forecasting or planning, if disclosure would prejudice the conduct of The LIC.
- Records of The LIC's intention in connection with negotiations with the individual, if disclosure might prejudice those negotiations.
- Various exemptions for certain crime and taxation purposes, where compliance with the provision would be likely to prejudice the crime or taxation purpose.