Data Protection Policy Statement

2021

DATA PROTECTION POLICY STATEMENT

Adopted / Late Reviewed:	October 2021
Review Period: **Next Review:**	3 Years October 2024
Contact Officer:	Emily McKenna, Head of Assurance
Policy Version:	Second version of policy
Version Reviewed by: **Version Approved by:**	CMT/ ELT / ARC
Policy Links:	Code of Conduct

Brief Policy Summary:
This policy sets out LHP's approach to Data Protection

Contents

1. Policy, Scope and Objectives

1.1 Members of the Board and Directors of Lincolnshire Housing Partnership (LHP), located at Westgate Park, Charlton Street, Grimsby, North East Lincolnshire are committed to compliance with all relevant UK and EU laws in respect of personal information and to protecting the fundamental rights and freedoms of natural persons whose information LHP collects, controls and processes in accordance with the UK General Data Protection Regulation (UK GDPR) as amended by the UK Data Protection Act 2018 (DPA 2018). To that end, the Members of the Board and Directors have developed, implemented, maintains and continuously improves a documented personal information management system ('PIMS') and Information Security Management Framework ('IMS') for LHP.

1.2 Scope

1.2.1 The scope of the PIMS & IMS takes into account the management responsibility, accountability, jurisdiction and geography. The PIMS includes any defined part of LHP

1.3 Objectives of the PIMS

1.3.1 LHP's objectives for the PIMS are that; it enables the organisation to meet its own and its data subjects requirements for the management of personal information; that it should support organisational objectives and obligations; that it should impose controls in line with LHP acceptable level of risk; that it should ensure that LHP meets applicable statutory, regulatory, contractual and/or professional duties; and that it should protect the interests ofnatural persons and other key stakeholders.

1.3.2 LHP is committed to complying with data protection legislation and good practice including:

a. processing personal information only where this is strictly necessary for legitimate organisational purposes;

b. collecting only the minimum specific personal information required for these purposes and not processing excessive personal information;

c. providing clear easy to understand information to individuals about how their personal information will be used and by whom;

d. only processing relevant and adequate personal information;

e. processing personal information fairly and lawfully;

f. maintaining an inventory of the categories of personal information processedby LHP;

g. keeping personal information accurate and, where necessary, up to date;

h. retaining personal information only for as long as is necessary for legal orregulatory reasons or, for legitimate organisational purposes;

i. respecting individuals' rights in relation to their personal information, includingtheir right of subject access;

j. keeping all personal information secure;

k. only transferring personal information outside the EU in circumstances whereit can be adequately protected;

l. the application of the various exemptions allowable by data protectionlegislation;

m. developing and implementing a PIMS to enable the policy to be implemented;

n. where appropriate, identifying internal and external stakeholders and thedegree to which these stakeholders are involved in the governance of LHP PIMS; and

o. the identification of employees with specific responsibility and accountabilityfor the PIMS.

2. Notification

2.1 LHP is registered with the Information Commissioner's Office (ICO) (registration number ZA345449) and declared that it processes the below information about data subjects.

2.2 We process personal information to enable us to provide social housing accommodation and services which include:

- letting, renting and leasing properties
- administering waiting lists
- carrying out research
- administering housing and property grants
- providing associated welfare services, advice and support
- maintaining our accounts and records
- supporting and managing our employees, agents, and contractors
- sale and purchase

- marketing

2.3 We also process personal information using CCTV systems to monitor and collect visual images for the purpose of security and the prevention and detection of crime.

2.4 We process information relevant to the above reasons/purposes. This information may include:

- personal details
- goods and services
- supplier details
- financial details
- lifestyle and social circumstances
- complaints
- education and employment details
- health, safety and security details
- visual images, personal appearance and behaviour
- family details
- member details

2.5 We also process sensitive classes of information that may include:

- physical or mental health details
- sexual life
- trade union membership
- offences and alleged offences
- criminal proceedings, outcomes and sentences
- racial or ethnic origin
- religious or other beliefs of a similar nature

2.6 We process personal information about:

- tenants
- applicants for accommodation which include their families andhouseholds
- asylum seekers
- business associates
- landlords
- local authority employees
- probation officers
- social workers
- spiritual and welfare advisers
- consultants and professional advisers
- survey respondents
- employees including self-employed contractors
- offenders and suspected offenders
- complainants and enquirers

- suppliers and service providers
- people captured by CCTV images

2.7 Where necessary or required we share information with:

- current, past or prospective employers
- family, associates and representatives of the person whose personaldata we are processing
- educators and examining bodies
- suppliers and service providers
- financial organisations
- central and local government
- auditors
- survey and research organisations
- other housing associations or trusts
- trade unions and associations
- health authorities and clinical commissioning groups
- enquirers and complainants
- security organisations
- health and social welfare organisations
- professional advisers and consultants
- the housing corporation
- probation services
- charities and voluntary organisations
- police forces
- courts and tribunals
- professional bodies
- employment and recruitment agencies
- credit reference agencies
- debt collection agencies
- landlords
- press and the media

2.8 LHP has identified all the personal data that it processes and this is contained in the Data Inventory Register.

2.9 A copy of the ICO notification details is retained by Data Protection Officer and the ICO Notification Handbook is used as the authoritative guidance for notification

2.10 The ICO notification is renewed annually on 18 April.

2.11 The Data Protection Officer is responsible, each year, for reviewing the details of notification in the light of any changes to LHP's activities (as determined by changes to the Data Inventory Register and the management review) and to any additional requirements identified by means of data protection impact assessments.

2.12 The policy applies to all Employees/Staff [and interested parties] of LHP. Any breach of the General Data Protection Regulation or this PIMS will be dealt with under LHP's disciplinary policy and may also be a criminal offence, in which case, the matter will be reported as soon as possible to the appropriate authorities.

2.13 Partners and any third parties working with or for LHP and who have, or may have, access to personal information, will be expected to have read, understood and to comply with this policy. No third party may access personal data held by LHP without having first entered into a data confidentiality agreement, which imposes on the third-party obligations no less onerous than those to which LHP is committed, and which gives LHP the right to audit compliance with the agreement.

3. Background to the General Data Protection Regulation ('GDPR') & UK Data Protection Act

3.1 The EU General Data Protection Regulation 2016 replaced the EU Data Protection Directive of 1995 and superseded the laws of individual Member States that were developed in compliance with the Data Protection Directive 95/46/EC. The UK's DPA 2018 was the UK's enactment of GDPR. At the end of 2020, when the UK ceased to be a member of the EU, the UK GDPR came into force, based on the EU GDPR and amended by the DPA 2018.

3.2 Its purpose is to protect the "rights and freedoms" of living individuals and to ensure that personal data is not processed without their knowledge, and, wherever possible, that it is processed with their consent.

4. Definitions Used by the Organisation (drawn from the GDPR)

4.1 **Territorial scope** – the GDPR will apply to all controllers that are established inthe EU (European Union) who process the personal data of data subjects, in the context of that establishment. It will also apply to controllers outside of the EU that process personal data in order to offer goods and services or monitor the behaviour to data subjects who are resident in the EU.

4.2 **Establishment** – the main establishment of the controller in the EU will be the place in which the controller makes the main decisions as to the purpose of its data processing activities. The main establishment of a processor in the EU will be its administrative centre. If a controller is based outside the EU, it will have to appoint a representative in the jurisdiction in which the controller operates, to act on behalf of the controller and deal with supervisory authorities.

4.3 **Personal data** – any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

4.4 **Special categories of personal data** – personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade-union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

4.5 **Data controller** – the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.

4.6 **Data subject** – any living individual who is the subject of personal data held by an organisation.

4.7 **Processing** – any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

4.8 **Profiling** – is any form of automated processing of personal data intended to evaluate certain personal aspects relating to a natural person, or to analyse, or predict that person's performance at work, economic situation, location, health, personal preferences, reliability, or behaviour. This definition is linked to the right of the data subject to object to profiling and a right to be informed about the existence of profiling, of measures based on profiling and the envisaged effects of profiling on the individual.

4.9 **Personal data breach** – a breach of security leading to the accidental, or unlawful, destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed. There is an obligation on the controller to report personal data breaches to the Information Commissioner's Office and where the breach is likely to adversely affect the personal data or privacy of the data subject.

4.10 **Data subject consent** - means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data.

4.11 **Third party** – a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data.

4.12 **Filing system** – any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis.

5. Responsibilities under the General Data Protection Regulation

5.1 LHP is a data controller and data processor asdefined under the GDPR.

5.2 Top Management and all those in managerial or supervisory roles throughout LHP are responsible for developing and encouraging good information handling practices within the organisation; responsibilities are set out in individual job descriptions.

5.3 The Data Protection Officer is accountable to Members of the Board and the Directors of LHP for the management of personal information within LHP and for ensuring that compliance with data protection legislation and good practice can be demonstrated. This accountability includes:

- development and implementation of the PIMS as required by this policy; and
- Security and risk management in relation to compliance with the policy.

5.4 The Data Protection Officer, who Members of the Board and the Directors considers suitably qualified and experienced, has been appointed to take responsibility for LHP's compliance with this policy on a day-to-day basis and, in particular, has direct responsibility for ensuring that LHP complies with the GDPR, as do Manager/Executive (generic/line) in respect of data processing that takes place within their area of responsibility.

5.5 The Data Protection Officer has specific responsibilities in respect of procedures such as the Subject Access Request Procedure and are the first point of call for Employees/Staff seeking clarification on any aspect of data protection compliance.

5.6 Compliance with data protection legislation is the responsibility of all members of LHP who process personal information.

5.7 LHP's Training Policy sets out specific training and awareness requirements in relation to specific roles and to members of LHP generally.

5.8 Members of LHP are responsible for ensuring that any personal data supplied by them, and that is about them, to LHP is accurate and up to date.

5.9 Where a meeting, training or other video call is to be recorded, the person leading the meeting will need to ask participants prior to the recording starting for permission; if any members refuse then the recording cannot take place. If all participants agree, the recording can begin and permissions reconfirmed with participants so that a record it kept. Recording should be stored securely, access limited and only kept for the specified time in the records retention policy.

6. Risk Assessment

6.1 Objective: To ensure that LHP is aware of any risks associated with the processing of particular types of personal information. LHP has a process for assessing the level of risk to individuals associated with the processing of their personal information.

6.2 Assessments will also be carried out in relation to processing undertaken by other organisations on behalf of LHP. LHP shall manage any risks which are identified by the risk assessment in order to reduce the likelihood of a non-conformance with this policy.

6.3 Where a type of processing, in particular using new technologies and taking into account the nature, scope, context and purposes of the processing is likely to result in a high risk to the "rights and freedoms" of natural persons, LHP shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data.

6.4 A single assessment may address a set of similar processing operations that present similar high risks.

6.5 Where, as a result of a Data Protection Impact Assessment, it is clear that LHP is about to commence processing of personal information that could cause damage and/or distress to the data subjects, the decision as to whether or not LHP may proceed must be escalated for review to the Data Protection Officer. The Data Protection Officer shall, if there are significant concerns, either as to the potential damage or distress, or the quantity of data concerned, escalate the matter to the Information Commissioner's Office.

6.6 Appropriate controls will be selected and applied to reduce the level of risk associated with processing individual data to an acceptable level, by reference to LHP's documented risk acceptance criteria and the requirements of the GDPR.

7. Data Protection Principles

7.1 All processing of personal data must be done in accordance with the following data protection principles of the Regulation and LHP Personal data must be processed lawfully, fairly and transparently.

7.2 The GDPR introduces the requirement for transparency whereby the controller has transparent and easily accessible policies relating to the processing of personal data and the exercise of individuals' "rights and freedoms". Information must be communicated to the data subject in an intelligible formusing clear and plain language.

7.3 The specific information that must be provided to the data subject must as a minimum include:

- the identity and the contact details of the controller and, if

any, of the controller's representative;

- the contact details of the Data Protection Officer, where applicable;
- the purposes of the processing for which the personal data are intended aswell as the legal basis for the processing;
- the period for which the personal data will be stored;
- the existence of the rights to request access, rectification, erasure or to object to the processing;
- the categories of personal data concerned;
- the recipients or categories of recipients of the personal data, whereapplicable;
- where applicable, that the controller intends to transfer personal data to arecipient in a third country and the level of protection afforded to the data;
- any further information necessary to guarantee fair processing.

7.4 Personal data can only be collected for specified, explicit and legitimate purposes.

7.5 Data obtained for specified purposes must not be used for a purpose that differs from those formally notified to the Information Commissioner as part of LHP's GDPR registration.

7.6 Personal data must be adequate, relevant, and limited to what is necessary for processing.

7.7 The Data Protection Officer is responsible for ensuring that information, which is not strictly necessary for the purpose for which it is obtained, is not collected.

7.8 All data collection forms (electronic or paper-based), including data collection requirements in new information systems, must be approved by the Data Protection Officer.

7.9 The Data Protection Officer will ensure that, on an annual basis all data collection methods are reviewed by internal audit/external experts to ensure that collected data continues to be adequate, relevant, and not excessive.

7.10 If data is given or obtained that is excessive or not specifically required by LHP's documented procedures, the Data Protection Officer is responsible for ensuring that it is securely deleted or destroyed in line with the Retention of Records Policy.

7.11 Personal data must be accurate and kept up to date.

7.12 Data that is kept for a long time must be reviewed and updated as necessary. No data should be kept unless it is reasonable to assume that it is accurate.

7.13 The Data Protection Officer is responsible for ensuring that all staff is trained in the importance of collecting accurate data and maintaining it.

7.14 It is also the responsibility of individuals to ensure that data held by LHP is

accurate and up to date. Completion of an appropriate registration or application form etc., will be taken as an indication that the data contained therein is accurate at the date of submission.

7.15 Employees/Staff/Customers/Others should notify LHP of any changes in circumstance to enable personal records to be updated accordingly. It is the responsibility of LHP to ensure that any notification regarding change of circumstances is noted and acted upon.

7.16 The Data Protection Officer is responsible for ensuring that appropriate additional steps are taken to keep personal data accurate and up to date, taking into account the volume of data collected, the speed with which it might change and any other relevant factors.

7.17 On at least an annual basis, the Data Protection Officer will review all the personal data maintained by LHP, by reference to the Data Inventory Register, and will identify any data that is no longer required in the context of the registered purpose and will arrange to have that data securely deleted/destroyed in line with Retention of Records Policy.

7.18 The Data Protection Officer is responsible for making appropriate arrangements that, where third party organisation's may have been passed inaccurate or out-of-date personal information, that the information is not to be used to make informed decisions about the individuals concerned; and for passing any correction to the personal information to the third party where this is required.

7.19 Personal data must be kept in a form such that the data subject can be identified only as long as is necessary for processing.

7.20 Where personal data is retained beyond the processing date, it will be minimised/encrypted/pseudonymised in order to protect the identity of the data subject in the event of a data breach.

7.21 Personal data will be retained in line with the retention of records procedure and, once its retention date is passed, it must be securely destroyed as set out in this procedure.

7.22 The Data Protection Officer must specifically approve any data retention that exceeds the retention periods and must ensure that the justification is clearly identified and in line with the requirements of the data protection legislation. This approval must be written.

7.23 Personal data must be processed in a manner that ensures its security

7.24 Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

7.25 These controls have been selected on the basis of identified risks to personal data, and the potential for damage or distress to individuals whose data is being

processed.

7.26 Security controls will be subject to audit and review.

7.27 Personal data is prohibited to be transferred to a country or territory outside the European Union or EEA

8. Accountability

8.1 The GDPR introduces the principle of accountability which states that the controller is not only responsible for ensuring compliance but for demonstrating that each processing operation complies with the requirements of the GDPR. Specifically, controllers are required to maintain necessary documentation of all processing operations, implement appropriate security measures, perform DPIAs (Data Processing Impact Assessment), comply with requirements for prior notifications, or approval from supervisory authorities and appoint a Data Protection Officer if required.

9. Data Subjects' Rights

9.1 Data subjects have the following rights regarding data processing and the data that is recorded about them:

- To make subject access requests regarding the nature of information held and to whom it has been disclosed
- To prevent processing likely to cause damage or distress
- To prevent processing for purposes of direct marketing
- To be informed about the mechanics of automated decision-taking process that will significantly affect them
- Not to have significant decisions that will affect them taken solely by automated process
- To sue for compensation if they suffer damage by any contravention of the GDPR
- To take action to rectify, block, erased, including the right to be forgotten, or destroy inaccurate data
- To request the ICO to assess whether any provision of the GDPR has been contravened
- The right for personal data to be provided to them in a structured, commonly used, and machine-readable format, and the right to have that data transmittedto another controller
- The right to object to any automated profiling without consent
- Data subjects may make data access requests as described in the Subject Access Request Procedure; this procedure also describes how LHP will ensure that its response to the data access requestcomplies with the requirements of the Regulation

10. Complaints

10.1 Data Subjects who wish to complain to LHP about how their personal information has been processed may lodge their complaint directly with the Data Protection Officer with guidance being available on the website or by phone call.

10.2 Data subjects may also complain directly to the Information Commissioner's Office and Data Protection Officer and LHP provides appropriate contact details.

10.3 Where data subjects wish to complain about how their complaint has been handled, or appeal against any decision made following a complaint, they may lodge a further complaint to the Data Protection Officer. The right to do this is included in the privacy policy under complaints procedure.

11. Consent

11.1 LHP understands 'consent' to mean that it has been explicitly and freely given, specific, informed, and unambiguous indication of the data subject's wishes by which he or she by statement, or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her. The consent of the data subject can be withdrawn at anytime.

11.2 LHP understands 'consent' to mean that the data subject has been fully informed of the intended processing and has signified theiragreement, while in a fit state of mind to do so and without pressure being exerted upon them. Consent obtained under duress or on the basis of misleading information will not be a valid basis for processing. There must be some active communication between the parties which demonstrate active consent. Consent cannot be inferred from non-response to a communication. For sensitive data, explicit written consent of data subjects must be obtained unless an alternative legitimate basis for processing exists.

11.3 In most instances consent to process personal and sensitive data is obtained routinely by LHP through contractual needs or when a new member of staff signs a contract of employment.

12. Security of Data

12.1 All Employees/Staff are responsible for ensuring that any personal data which LHP holds and for which they are responsible, is kept securely and is not under any conditions disclosed to any third party unless that third party has been specifically authorised by LHP to receive that information and has entered into a confidentiality agreement.

12.2 All personal data should be accessible only to those who need to use it and access may only be granted in line with the Access Control Policy. Individuals should form a judgment based upon the sensitivity and value of the information in question, but personal data must be kept:

- in a lockable room with controlled access; and/or
- in a locked drawer or filing cabinet; and/or
- if computerised, password protected in line with corporate requirements in the Access Control Policy

12.3 Care must be taken to ensure that PC screens and terminals are not visible except to authorised Employees/Staff of LHP (ISP3). All Employees/Staff are required to enter into an Acceptable Use Agreement (before they are given access to organisational information of any sort).

12.4 Manual records may not be left where they can be accessed by unauthorised personnel and may not be removed from business premises without explicit written authorisation. As soon as manual records are no longer required for day- to-day client support, they must be removed from secure archiving in line with the Records Retention Policy.

12.5 Personal data may only be deleted or disposed of in line with the Data Retention Procedure. Manual records that have reached their retention date are to be shredded and disposed of as 'confidential waste'. Hard drives of redundant PCs are to be removed and immediately destroyed as required before disposal.

12.6 Processing of personal data 'off-site' presents a potentially greater risk of loss, theft or damage to personal data. Staff must be specifically authorised to process data off-site.

13. Rights of Access to Data

13.1 Data subjects have the right to access any personal data (i.e., data about them) which is held by LHP in electronic format and manual records which form part of a relevant filing system. This includes the right to inspect confidential personal references received by LHP and information obtained from third-party organisations about that person.

14. Disclosure of Data

14.1 LHP must ensure that personal data is not disclosed to unauthorised third parties which includes family members, friends, government bodies and in certain circumstances, the Police. All Employees/Staff should exercise caution when asked to disclose personal data held on another individual to a third party. It is important to bear in mind whether or not disclosure of the information is relevant to, and necessary for, the conduct of LHP's business.

14.2 The GDPR permits certain disclosures without consent so long as the information is requested for one or more of the following purposes:

- to safeguard national security;
- prevention or detection of crime including the apprehension or prosecution ofoffenders;
- assessment or collection of tax duty;

- discharge of regulatory functions (includes health, safety and welfare of persons at work);
- to prevent serious harm to a third party;
- to protect the vital interests of the individual, this refers to life and death situations.

14.3 All requests to provide data for one of these reasons must be supported by appropriate paperwork and all such disclosures must be specifically authorised by the Data Protection Officer.

15. Retention and Disposal of Data

15.1 Personal data may not be retained for longer than it is required. Once a member of staff has left LHP, it may not be necessary to retain all the information held on them. Some data will be kept for longer periods than others. LHP's data retention and data disposal procedures will apply in all cases.

16. Disposal of Records

16.1 Personal data must be disposed of in a way that protects the "rights and freedoms" of data subjects (e.g., shredding, disposal as confidential waste, secure electronic deletion) and in line with the secure disposal procedure

17. Document Owner and Approval

17.1 The Data Protection Officer is the owner of this document and is responsible for ensuring that this procedure is reviewed in line with the review requirements of the GDPR.

17.2 This policy was approved by Members of the Board and the Directors and is issued on a version-controlled basis under the signature of the Chief Executive.

Signature: