Data Protection Policy

2025

DATA PROTECTION POLICY

Adopted / Last Reviewed:	April 2025
Review Period: **Next Review:**	3 Years April 2028
Contact Officer:	Nicola Ebdon, Executive Director of Governance and Regulation & LHP's Data Protection Officer
Policy Version:	Third version of policy
Target Audience:	LHP Colleagues & Customers
Version Reviewed by: **Version Approved by:**	Leadership Team, 26 March 2025 Audit & Risk Committee, 30 April 2025
Policy Links:	Code of Conduct Whistleblowing Policy Complaints Policy Information Systems Security Policy Privacy Policy

Brief Policy Summary:

This policy sets out LHP's approach to Data Protection for LHP colleagues and customers. It should be read together with our website page Your Data – Your Rights and our Privacy Policy which includes information on:

- What is personal data
- Data we may collect
- How we use data
- How we may share data
- How long we keep data
- How we keep data safe
- Transfers to other countries
- Data subjects' rights

Contents

Background, Scope and Objectives

Background

1. Lincolnshire Housing Partnership ("**LHP**") needs to collect and process personal data about people with whom it deals to carry out business and provide services. Such people include – but are not limited to – LHP customers, colleagues, Non-Executive Directors and third parties.

2. Non-Executive Directors of the Board and Executive Directors of LHP are committed to complying with the applicable Data Protection Legislation, good Data Protection practice and the Data Protection Principles, to protect the fundamental rights and freedoms of data subjects whose information LHP collects, controls and processes in accordance with applicable Data Protection Legislation. The Data Protection principles are explained on our website and Basecamp page.

3. The applicable Data Protection Legislation includes – but is not limited to – the UK General Data Protection Regulation ("**UK GDPR**") and the UK Data Protection Act 2018 ("**DPA 2018**"), the Privacy and Electronic Communications Regulations (2003) ("**PECR**"), the Telecommunications (Lawful Business Practice)_ (Interception of Communications) Regulations 2000 and the proposed – but not yet implemented – Social Tenant Access to Information Requirements ('**STAIR**') and Data Protection and Digital Information Bill.

4. The UK GDPR's purpose is to protect the "rights and freedoms" of data subjects and ensure that personal data is not processed without their knowledge and, wherever possible, that it is processed with their consent.

5. In addition, various guidelines, codes of practice and case law contribute to the Data Protection Legislation. It is also possible that LHP is subject to the EU GDPR and other European (and non-European) legislation.

6. For the definitions (and meanings) of various terms used within this Policy, please refer to Appendix A.

Scope

7. The policy applies to all colleagues, customers and interested parties of LHP. Any breach of the UK GDPR or this Policy will be dealt with in accordance with LHP's Disciplinary Policy and may also be a criminal offence, in which case, the matter will be reported to the appropriate authorities.

Objectives of this Policy

8. It enables LHP to meet requirements for the management of personal information and ensures that LHP meets applicable statutory, regulatory, contractual and/or professional duties; and protects the interests of data subjects.

Notification (with the ICO)

9. LHP is registered with the Information Commissioner's Office ("**ICO**") (registration number ZA345449) and renews its annual ICO registration fee on (or around) 18 April

each calendar year. A copy of the ICO notification is retained by the Data Protection Officer and the ICO's Register is used as the authoritative guidance for notification. The Data Protection Officer is responsible for reviewing the details of notification in the light of any changes to LHP's activities and any additional requirements identified by Data Protection impact assessments.

10. LHP has identified all the personal data that it processes, and this is contained in the Record of Processing Activity. Further information on the personal data which LHP collects, processes, stores, transfers or shares, and the reasons for processing, is provided on our website and BaseCamp page.

11. 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 comply with this policy. No third party may access personal data held by LHP without having entered into a data processing or sharing 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.

Responsibilities under the UK GDPR

12. LHP is a data controller and Data Processor as defined under the UK GDPR.

13. Senior Leadership and all those in managerial or supervisory roles throughout LHP are responsible for developing and encouraging good information handling practices within LHP.

14. The Data Protection Officer is accountable to Non-Executive Directors of the Board and the Executive 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 includes ensuring compliance with the Data Protection Principles.

15. The Data Protection Officer, who the Board and the Executive 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 Managers/Executives (generic/line) in respect of data processing that takes place within their area of responsibility.

16. The Data Protection Officer has specific responsibilities in respect of procedures such as the Data Breach and the Subject Access Request Procedure and together with the Data Protection Business Partner is the first point of call for colleagues and customers seeking clarification on any aspect of Data Protection compliance. This includes:

    - ensuring appropriate steps are taken to keep personal data accurate and up to date, considering the volume of data collected, the speed with which it might change and any other relevant factors; and
    - ensuring routine review all the personal data maintained by LHP, by

reference to the Record of Processing Activity, and identification any data that is no longer required in the context of the registered purpose for secure deletion/destruction in line with the Records Retention Schedule.

17. Compliance with Data Protection legislation is the responsibility of all who process personal information at LHP. This includes:

    - colleagues;
    - apprentices, agency workers, trainees, any third-party contractor whose work is controlled by LHP (other than a genuinely self-employed person); and
    - other people involved with LHP, for example, Board and Committee Non-Executive Directors, Trainee Non-Executive Directors or involved customers.

18. All colleagues should complete specific training on Data Protection and ensure they continue to be aware of Data Protection requirements.

19. All LHP colleagues and customers are responsible for ensuring that any personal data supplied by them, and that is about them, to LHP is accurate and up to date.

20. 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 is kept. Recording should be stored securely, access limited and only kept for the specified time in the records retention policy.

Data Protection Impact Assessments

21. LHP conducts Data Protection Impact Assessments (DPIAs) to identify, analyse and mitigate risks to data subjects when processing personal data. This ensures LHP adequately manages (by way of controls or other mitigation factors) any risks to data subjects associated with the processing of personal data. Separate DPIAs will be completed for any (and all) processing activities undertaken by LHP.

22. 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 to reduce the likelihood of a non-conformance with this policy.

23. 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 data subjects, LHP shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data.

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

25. Where, as a result of a DPIA, it is clear that LHP is about to commence processing of personal information that could cause damage and/or distress to data subjects, the decision as to whether or not LHP may proceed must be escalated for review to the Data Protection Officer.

26. 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 UK GDPR.

Data Protection Principles

27. The UK GDPR sets out key principles which are further explained on our website. LHP will ensure that it adheres to the principles to ensure Data Protection compliance, that personal data is processed lawfully, fairly and transparently, and data processing risks are minimised.

28. The UK GDPR includes a requirement to ensure transparent and easily accessible policies relating to the processing of personal data and the exercise of individuals' "rights and freedoms". Information must be communicated in an intelligible form using clear and plain language. Specific information that must be provided to data subjects must as a minimum include:

    - the identity and contact details of the controller and, if any, 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 as well 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, where applicable;
    - where applicable, that the controller intends to transfer personal data to a recipient in a third country and the level of protection afforded to the data; and
    - any further information necessary to guarantee fair processing.

Lawful basis for Data Processing

29. The lawful bases for data processing are set out in Article 6 of the UK GDPR, and at least one of these must apply whenever LHP processes personal data. The lawful basis for processing must be recorded in the associated DPIA. Many of the

lawful bases for processing depend on the Data Processing being “necessary” – however, this does not mean that the processing must be essential.

30. Data Processing must be a targeted and proportionate way of achieving a specific purpose – and a lawful basis will not apply if LHP can reasonably achieve the purpose by some other (less intrusive) means, or by processing less personal data.

31. LHP must be able to demonstrate that:

    - there has been a full and complete consideration of which lawful basis (or bases) apply to each Data Processing undertaken;
    - this has been recorded adequately, for audit trail purposes (and if required by the Regulator);
    - any (and all) decisions made, and record-keeping, has an appropriate person (or persons) assigned as ‘responsible’ and ‘accountable’. This is likely to be recorded on the finalised DPIA document for the process under consideration; and
    - it has communicated the lawful basis (or bases) for Data Processing to the Data Subjects involved in (or affected by) the process under consideration.

32. If Data Processing purposes change over time, or there is – or may be – a new purpose which was not originally anticipated, LHP must comply with the purpose limitation principle and ensure:

    - the new purpose is compatible with the original purpose, or
    - the Data Subject’s (or Subjects’) specific consent for the new purpose is obtained, or
    - LHP can justify a clear legal provision requiring or allowing the new processing in the public interest (this may be an unlikely, or inappropriate, option).

33. Our website contains further details on the categories of personal data that are processed by LHP, and the reason(s) for doing so.

International Data Transfers / Restricted Transfers

34. An international/restricted data transfer refers to the process of moving or sharing personal data from the UK to a country or recipient (either a Data Processor, or a Joint Data Controller) outside of the UK.

35. Personal data should only be transferred outside the UK where it is strictly necessary to do so. Prior to transferring any personal data outside of the UK, LHP will take steps to ensure that an appropriate risk assessment (known as a transfer risk assessment) has been completed (and recorded for file), and there are appropriate international data transfer mechanisms in place to safeguard the data. These safeguards should be discussed with the Data Protection Officer.

Data Subjects' Rights

36. Data subjects have several rights under law in regard to Data Processing and the data that is recorded about them. Information and procedures for data subjects rights are explained on LHP's website and Data Protection BaseCamp page.

Complaints

37. Data Subjects may complain about the way LHP has accessed their information, how LHP has handled (or processed) their personal data – or other people's data (if they have relevant authority or consent), internet search results, and – where applicable – CCTV footage recorded.

38. Data Subjects who wish to complain to LHP about how their personal information has been processed may complain by completing our online form on our website or phoning our customer service advisors on 0345 604 1472.

39. Complaints made to LHP will be managed in accordance with LHP's Complaints Policy.

40. If, following the issue of LHP's final response letter to a complaint, a Data Subject is not happy with the response provided, they may refer the complaint to the ICO. This may be done using the ICO's online form, or via telephone.

Consent

41. One of the lawful bases for processing personal data is consent. In order to be valid, it must be explicitly and freely given, specific and unambiguous. The Data Subject must have been fully informed of the intended processing and signified their agreement, while in a fit state of mind to do so and without pressure being exerted upon them. Consent obtained under duress or based on misleading information will not be valid. Consent cannot be inferred from non-response to a communication.

42. A Data Subject can withdraw their consent at any time. If a Data Subject withdraws their consent, this does not affect the lawfulness of the processing up to that point. However, any subsequent Data Processing must stop (if it was solely based on consent).

Security of Data

43. All colleagues 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 data processing or sharing agreement.

44. All personal data should be accessible only to those who need to use it and personal data must be kept safe

45. in accordance with the Information Systems Security Policy. Manual records may not be left where they can be accessed by unauthorised personnel and may not

be removed from business premises without 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.

46. Processing of personal data 'off-site' presents a potentially greater risk of loss, theft or damage to personal data. Colleagues must be specifically authorised to process data off-site and contractors and sub-contractors can only process if a data processing agreement is signed.

Data Breaches

47. All colleagues with access to personal data for which LHP is either data controller or processor must report all personal data breaches using the online form on BaseCamp or by emailing Data.protection@lincolnshirehp.com as soon as they become aware of the breach (whether this is actual or suspected). LHP logs all personal data breaches and will investigate each incident without delay. Appropriate remedial action will be taken as soon as possible to isolate and contain the breach, evaluate and minimise its impact, and to recover from the effects of the breach. Data Protection near misses should also be reported and will be investigated in the same manner as Data Protection breaches.

Disclosure of Data

48. LHP must ensure that personal data is not disclosed to unauthorised third parties unless there is a data processing or sharing agreement in place, or it is necessary to do so and there is a clear lawful basis (likely to be vital interests, legitimate interests or a legal obligation). All colleagues should exercise caution when asked to disclose personal data to a third party and seek advice from Data Protection before sharing personal data.

49. The UK GDPR permits certain disclosures without consent for a variety of reasons, which may include – but are not limited to – the following:

- safeguard national security;
- prevention or detection of crime including the apprehension or prosecution of offenders;
- assessment or collection of tax duty;
- discharge of regulatory functions (includes health, safety and welfare of persons at work);
- prevent serious harm to a third party; or
- protect the vital interests of the individual, this refers to life and death situations.

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

51. Where LHP shares personal data with third parties such as law enforcement, we make sure that we have a lawful basis for disclosure. If the personal data concerned is special category data, we make sure that an Article 9 UK GDPR condition (as well as the Article 6 basis) applies.

52. Where LHP shares data with Data Processors, we carry out appropriate due diligence and ensure there is an adequate Data Sharing or Processing Agreement in place prior to any personal data sharing.

Retention and Disposal of Personal Data

53. LHP's Records Retention Policy provides information on data retention and data disposal. Personal data **must** be deleted or disposed of in line with the Records Retention Policy and in a way that protects the "rights and freedoms" of data subjects (e.g., shredding, disposal as confidential waste, secure electronic deletion). Manual records that have reached their retention date are to be shredded and disposed of as 'confidential waste'.

54. Personal data may not be retained for longer than required. With the DPO's written approval, Personal data may be retained for longer than this – but LHP must ensure the justification is clearly identified and in line with the requirements of the appropriate Data Protection Legislation.

Direct Marketing

55. Direct marketing includes all the processing of personal data that leads up to, directly enables or supports sending any direct marketing messages. Direct marketing may take various forms including: emails, text messages, phone calls, post, online advertising and social media marketing.

56. LHP is subject to certain obligations under the UK GDPR, Data Protection Act 2018 and, when applicable, the Privacy and Electronic Communications Regulation 2003 ("PECR") when undertaking direct marketing activities to LHP customers or other data subjects, which involves the processing of personal data. LHP will follow the ICO's Guidance on Direct Marketing, to ensure appropriate compliance.

57. Data subjects have the right to object to (or withdraw consent already provided) direct marketing. If a data subject opts out at any time, their details will be suppressed as soon as possible. Suppression involves retaining just enough information to ensure that direct marketing preferences (i.e. an objection to, or withdrawal of consent from, direct marketing) are respected in the future. If a Data Subject subsequently changes their mind to direct marketing, then LHP will make the appropriate amendments to the suppression lists maintained.

APPENDIX A – DATA PROTECTION DEFINITIONS USED

The following terms used within this Policy have the following meanings:

Term	Definition (meaning)
Data Subject	Any living individual who is the subject of personal data held by an organisation (in this case, LHP). A data subject is someone who can be identified from Personal data. This means that anyone who had died is not classed as a 'data subject' and is not subject to the UK GDPR.
Personal Data	Any information relating to a data subject; who can be identified directly or indirectly, 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.
Special Categories of Personal Data ('**SCD**')	The UK GDPR singles out the following types of personal data as likely to be more sensitive and gives them extra protection: racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data (where used for identification purposes), health, sex life and sexual orientation.
Data Controller ('**DC**')	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. DCs make decisions about processing activities. They exercise overall control of the personal data being processed and are ultimately in charge of and responsible for the processing.
Data Processor ('**DP**') (sometimes referred to as 'Third-Party')	Data Processor means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the Data Controller. DPs act on behalf of the relevant Data Controller and under their authority. In doing so, they serve the Data Controller's interests, rather than their own.
Data Processing	This means taking any action with a Data Subject's personal data. This includes 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.
Personal Data Breach ('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.
Consent	This means any unambiguous statement (or clear affirmative action) that has been freely given, is specific and from an informed position of the data subject's agreement to the data processing to be undertaken.
Lawful basis	Whenever personal data is processed, there must be a valid reason for doing so – and this is known as a 'lawful basis'. There are six lawful bases, as follows: • Consent • Contractual obligations • Legal obligations • Vital interests • Public task (in the public interest) • Legitimate interests None of the lawful bases are better or more important than any of the others. The most appropriate one (or ones) must be identified for the data processing being undertaken – and there may be different lawful bases for each different data processing undertaken.
Individual (or data subject's) rights	In Data Protection law, people have rights over their data, which include the right: • to be informed (about the collection and use of Personal data); • of access (to personal data); • to rectification (of inaccurate personal data and to update incomplete personal data);

	• to erasure; • to restrict processing; • to data portability; • to object (to data processing); and • rights in relation to automated decision making and profiling.
Profiling	This is any form of automated processing of Personal data intended to evaluate certain personal aspects relating to a data subject, 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 data subject.
Data Protection Impact Assessment ("**DPIA**")	A DPIA is a process to help LHP identify and minimise the Data Protection risks of a project, service, product, or task – anything that involves processing Personal data. A DPIA must be completed for any Data Processing that is likely to result in a high risk to Data Subjects – and this includes some specified types of processing.

Lincolnshire Housing Partnership (LHP)

Equality and Quality Impact Assessment (EQIA)

Title of Policy/Event/Decision: Data Protection Policy

Lead Officer(s): Executive Director of Governance & Regulation

Date of EQIA: 01 April 2025

Scope and Purpose	
Briefly describe the policy/event/decision being assessed:	This policy sets out LHP's approach to Data Protection for both LHP colleagues and customers.
What is the aim or purpose of this policy/decision?	It enables LHP to meet requirements for the management of personal information and ensure that LHP meets applicable statutory, regulatory, contractual and/or professional duties; and protects the interests of data subjects.
Which departments or groups will be affected by this policy/event/decision?	LHP colleagues and customers – including Board and Committee members and involved customers.
Data Collection and Evidence	
What data or evidence have you used to identify how different groups may be affected? (e.g., tenant demographic data, service usage statistics, consultation feedback)	We have customer diversity monitoring data so we understand the demography of this set of data subjects and have taken this into consideration. We are awaiting colleague diversity monitoring data to be able to consider this. We have low number of colleagues and customers subject to data breaches or subject access requests – however commit to analyse the data available on an annual basis to identify any impacts on these specific elements of Data Protection compliance.
What does this data tell you about the potential impacts on different equality groups?	[Awaiting summary of customer demographics] There is a risk that Data Protection information or procedures may be perceived as intimidating or inaccessible for people from under-represented groups or with particular needs (e.g. neurodiverse members, those with mental health concerns).

RAG Impact Assessment on Protected Characteristics					
Use the RAG system to assess the level of potential impact for each protected characteristic: • **Red (High Risk):** Significant potential for negative impact requiring immediate action to mitigate. • **Amber (Medium Risk):** Some potential for negative impact, which can be mitigated with changes. • **Green (Low or No Risk):** Little to no negative impact identified. Ensure that you state reasons (the why) for your justifications.					
Protected Characteristic	**Impact (Positive, Negative, Neutral)**	**RAG Rating**	**Description of Potential Impact**	**Mitigation/ Enhancement Actions**	**Responsible Officer**
Age	Neutral		Policy is role based, not age based. No age barriers identified	N/A	N/A
Disability	Potential Barrier		Information in the policy/ website or processes may be stressful or inaccessible	Offer reasonable adjustments, use plain English and accessible formats	CHoGR
Gender Reassignment	Neutral		No direct impact identified	Maintain inclusive culture, use appropriate pronouns in correspondence	CHoGR
Marriage and Civil Partnership	Neutral		No impact anticipated	N/A	N/A
Pregnancy and maternity	Neutral		No impact anticipated	N/A	N/A
Race	Neutral		No impact anticipated	N/A	N/A

Religion or Belief	Neutral		No impact anticipated	N/A	N/A
Sex	Neutral		No identified impact	N/A	N/A
Sexual Orientation	Neutral		No identified impact	N/A	N/A

Mitigating Negative Impact	
What actions will you take to reduce or mitigate any identified negative impacts? Provide specific mitigation measures for each characteristic where a negative impact (Red or Amber rating) was identified.	Mitigation measures have been identified to ensure adjustments to accessibility are made where necessary. The policy has been reviewed to limit the use of legal language where possible – and a supporting communications campaign has been developed to enable customers to become more aware of key information. Data Protection training has been designed for colleagues to explain terms and ensure relevance to roles and LHP. Analysis will be completed on data breaches and subject access requests to ensure no adverse effect on underrepresented groups.
Who is responsible for implementing these actions?	Corporate Head of Governance & Regulation
Consultation and Engagement	
Have you consulted any stakeholders or equality groups? If so, who and how?	Customer Forum, Leadership Team to review the whole policy – ahead of approval by the Audit & Risk Committee.
What feedback have you received, and how has this influenced your assessment?	The Customer Forum provided feedback which reinforced the importance of providing accessible information on Data Protection rights, including the right to access, rectification, and objection to processing. Customers also stressed the need for non-digital communication channels, leading to the recommendation of a dedicated Data Protection section in our quarterly magazine.

Decision Making	
How has this EQIA informed or influenced the final decision?	The EQIA helped ensure the policy included: • accessible information; and • commitment to reasonable adjustments under the Equality Act 2010
Were any changes made to the policy/decision as a result of the EQIA?	Reinforced the need for accessible communications – and a commitment to complete diversity monitoring on data breaches and subject access requests.
Monitoring and Review	
How will you monitor the actual impact of the policy/decision once it is implemented?	Data subjects involved with data breaches and subject access requests will be monitored and analysed by the Data Protection Business Partner annually to assess impacts.
When will the policy/ decision be reviewed?	April 2028. Interim reviews will occur if the regulatory framework or feedback indicates the need for amendment.
Sign-Off **EQIA Completed By:** *Lead Officer(s) Name(s):* *Date:*	Executive Director of Governance & Regulation 03/04/25
Approved By: *Approval Name:* *Date:*	awaited