Data Protection Policy

Approval date – March 2018
Review date – March 2021

This policy will take effect on 25 May 2018

This policy applies to

☑ Link Group	☑ Link Housing	☑ Link Living	☑ Link Property
☑ Horizon	☑ Larkfield	☑ West Highland	☑ Lintel Trust

Policy Summary

This policy reflects the changes to data protection legislation following the introduction of the General Data Protection Regulation [GDPR] on 25 May 2018. The legislation enhances the provisions laid out in the Data Protection Act 1998 and requires organisations to be able to demonstrate accountability with the six data protection principles.

Equalities

This policy fully complies with Link's Equality, Diversity and Inclusion Policy and no impact on any of the protected characteristics has been identified.

Privacy

This policy covers Link's policy on data protection following the introduction of the General Data Protection Regulation which enhances the rights of data subjects and provides stricter guidelines for organisations to follow.

Policy Owner	**Review Manager**	**Approved By**
Director of Human Resources and Business Support	Strategy and Business Support Manager	Link Group Board

Revision History		
Date	Version Number	Comments
19/03/2018	1	

1. INTRODUCTION

1.1 The Link group of companies is committed to ensuring the secure and safe management of data held by Link in relation to customers, staff and other individuals. Link staff have a responsibility to ensure compliance with the terms of this policy and to manage individuals' data in accordance with the procedures outlined in this policy and associated documentation.

1.2 Link needs to gather and use certain information about individuals. They can include customers (tenants, factored owners, service users and participants), employees and other individuals with whom Link has a relationship. Link manages a significant amount of data from a variety of sources. This data contains Personal and Special Categories of Personal Data (the latter previously known as 'Sensitive Data').

1.3 This policy sets out Link's duties in processing that data and the purpose of this policy is to set out procedures of managing of such data.

2. LEGISLATION

2.1 It is a legal requirement that Link processes data correctly. Link must collect, handle and store personal data or special categories of personal data in accordance with the relevant legislation.

2.2 The relevant legislation in relation to the processing of data is:

a) the General Data Protection Regulation (EU) 2016/679;

b) the Privacy and Electronic Communications (EC Directive) Regulations 2013 (as may be amended by the proposed Regulation on Privacy and Electronic Communications); and

c) any legislation that, in respect to the United Kingdom, replaces, or enacts into United Kingdom domestic law, the General Data Protection Regulation (EU) 2016/679, the proposed Regulation on Privacy and Electronic Communications or any other law relating to data protection, the processing of personal data and privacy as a consequence of the United Kingdom leaving the EU.

3. DATA

3.1 Link holds a variety of data relating to individuals, including customers and employees (also referred to as data subjects) which is known as Personal Data. The Personal Data held and processed by Link is detailed within the Fair Processing and Privacy Notice and the Data Protection Addendum to the Terms and Conditions of Employment which has been provided to all employees.

3.1.1 "Personal Data" is that from which a living individual can be identified either by the data alone or in conjunction with other data held by Link.

3.1.2 Link also holds Personal data that is sensitive in nature (i.e. relates to or reveals a data subject's racial or ethnic origin, religious beliefs, political opinions, medical conditions or sexual orientation). This is "Sensitive Data".

4. PROCESSING OF PERSONAL DATA

4.1 Link is permitted to process Personal Data on behalf of data subjects provided it is doing so on one of the following grounds:

- Consent of the data subject;
- Processing is necessary for the performance of contract between Link and the data subject or for entering into a contract with the data subject;
- Processing is necessary for Link's compliance with a legal obligation;
- Processing is necessary to protect the vital interests of the data subject or another person;
- Processing is necessary for the performance of a task carried out in the public interest or in the exercise of Link's official authority; and
- Process is necessary for the purposes of legitimate interests

4.2 Fair Processing Notice

4.2.1 Link has produced a Fair Processing Notice which it is required to provide to all customers whose Personal Data is processed by the organisation. That Fair Processing Notice will be provided to the customer prior to processing their Personal Data and they will be advised of the terms of the Fair Processing Notice when it is provided to them.

4.3 Employees

4.3.1 Employees' Personal Data and, where applicable, Sensitive Personal Data, is held and processed by Link. Details of the data held and processing of that data is supplied to employees at the same time as their Contract of Employment.

4.4 Consent

From time to time, Link will need to obtain specific consent to process an individual's personal data. This will happen in situations where no other permitted grounds for processing the information are available. Where consent is required, the individual data subject will be asked to confirm in writing that they freely consent to allowing their data to be processed for that specific and defined purpose. General consent to data processing cannot be sought or legally relied upon.

4.5 Processing of Sensitive Personal Data

In the event that Link processes Sensitive Personal Data, it must do so in accordance with one of the following grounds:

- The data subject has given explicit consent to the processing of this data for a specific purpose

- Processing is necessary for carrying out obligations or exercising rights related to employment or social security
- Processing is necessary to protect the vital interests of the data subject or , if the data subject is incapable of giving consent, the vital interests of another person
- Processing is necessary for the establishment, exercise or defence of legal claims, or whenever courts are acting in their judicial capacity; and
- Processing is necessary for reasons of substantial public interest.

5. DATA SHARING

5.1 Link shares its data with various third parties for numerous reasons so that its day to day activities are carried out in accordance with relevant policies and procedures. In order that Link can monitor compliance by these third parties with Data Protection law, Link will require the third party to enter into an agreement governing the processing of data, security measures to be implemented and responsibilities for breaches.

5.2 Data Sharing

5.2.1 Personal Data is from time to time shared amongst Link and third parties who require to process personal data that Link processes as well. Both Link and the third party will be processing that data in their individual capacity as data controllers.

5.2.2 Where Link shares in the processing of personal data with a third party organisation (e.g. for processing of an employee's pension), it shall require the third party organisation to enter into a Data Sharing Agreement with Link in accordance with the terms of the model Data Sharing Agreement set out in Appendix 3 to this Policy.

5.3 Data Processors

A data processor is a third party entity that processes personal data on behalf of Link, for example, frequently outsourced work such as cyclical maintenance and, gas servicing repairs work.

5.3.1 A data processor must comply with Data Protection laws. Link's data processors must ensure they have appropriate technical security measures in place, maintain records of processing activities and notify Link if a data breach is suffered. Link will enter into Data Processing Agreements with each data processor which sets out their obligations under data protection legislation.

5.3.2 If a data processor wishes to sub-contract their processing, prior written consent of Link must be obtained. Upon a sub-contracting of processing, the data processor will be liable in full for the data protection of their sub-contractors.

5.3.3 Where Link contracts with a third party to process Personal Data held by Link, it shall require the third party to enter into a Data Processing Agreement. This process will be overseen by the relevant director to ensure their business area is compliant.

6. DATA STORAGE AND SECURITY

All Personal Data held by Link must be stored securely, whether electronically or in paper format.

6.1 Paper Storage

If Personal Data is stored on paper it will be kept in a secure place where unauthorised personnel cannot access it. When the Personal Data is no longer required it will be disposed of by the employee so as to ensure its destruction. If the Personal Data requires to be retained on a physical file then the employee should ensure that it is affixed to the file which is then stored in accordance with Link's Data Retention Schedule.

6.2 Electronic Storage

Personal Data stored electronically must also be protected from unauthorised access. Access to Personal Data will be controlled and organised according to the principle of least privilege. Personal Data will always be encrypted in transit and at rest. Any Personal Data sent externally to Link's data processors or those with whom Link has entered into a Data Sharing Agreement will, therefore, be encrypted. Personal data must never be stored on portable storage devices (CD, DVD, USB memory stick, external hard drive etc). Personal Data must only be stored in secure locations as directed by the Information Management Strategy.

7. BREACHES

7.1 A data breach can occur at any point when handling Personal Data and Link has reporting duties in the event of a data breach or potential breach. Breaches which pose a risk to the rights and freedoms of the data subjects who are subject to the breach require to be reported externally in accordance with Clause 7.3 below.

7.2 Internal Reporting

Link takes the security of data very seriously and, in the unlikely event of a data breach, will take the following steps:

- Assemble the Data Breach Response Team as per the Data Breach Response Plan which sits alongside the Business Continuity Plan, ICT Disaster Recovery Plan and the Crisis Communications Plan.
- Liaise with Link's Data Forensic Contractor and Cyber Insurance provider
- Establish contact with the Information Commissioner's Office to report the breach with 72 hours of the breach being identified

7.3. Reporting to the Information Commissioner's Office [ICO]

Link requires to report any breaches which pose a risk to the rights and freedoms of the data subjects which are subject to the breach to the ICO within 72 hours of the breach occurring (this includes weekends). Link will also consider whether it is appropriate to notify those data subjects affected by the breach.

8. DATA SUBJECT RIGHTS

8.1 Enhanced existing rights and new rights are provided to data subjects under the GDPR. They are entitled to view the personal data held about them by Link, where in written or electronic form.

8.2 Data subjects now have a right to request a restriction of processing their data, a right to be forgotten and a right to object to Link's processing of their data. These rights are notified to Link tenants and other customers in the Fair Processing Notice.

8.3 Subject Access Requests

Data subjects are permitted to view their data held by Link upon making a request to do so (a subject access request). Upon receipt of a request by a data subject, Link must respond to the request within one month of receiving the request. Link's Subject Access Request procedure is available on Linkipedia here. Link:

8.3.1 must provide the data subject with an electronic or hard copy of the personal data requested, unless any exemption to the provision of that data applies in law.

8.3.2 must take reasonable steps to obtain consent from those data subjects to the disclosure of that personal data where the personal data comprises data relating to a third party. If no consent is obtained then no personal data relating to a third party may be disclosed.

8.3.3 must confirm to the data subject as soon as practically possible where it does not hold the personal data sought by the data subject and in any event, no later than one month from the date on which the request was received.

8.4 **Right to be Forgotten**

8.4.1 A data subject may exercise their right to be forgotten by submitting a request in writing to Link that it erase the data subject's Personal Data in its entirety.

8.4.2 Each request received by Link will require to be considered on its own merits and legal advice will require to be obtained in relation to such requests from time to time.

8.5 **The Right to Restrict or Object to Processing**

8.5.1 A data subject may request that Link restrict its processing of the data subject's Personal Data, or object to the processing of that data. In the event that any direct marketing is undertaken by Link, a data subject has an absolute right to object to processing of this nature, and if Link receives a written request to cease processing for this purpose, then it will do so immediately.

8.5.2 Each request received by Link will require to be considered on its own merits and legal advice will require to be obtained in relation to such requests from time to time.

9. PRIVACY IMPACT ASSESSMENTS (PIA)

9.1 These are a means of helping Link to identify and reduce the risks that its operations have on the personal privacy of data subjects.

9.2 Link shall:

9.2.1 Carry out a PIA before undertaking a project or processing activity which poses a "high risk" to an individual's privacy. High risk can include, but is not limited to, activities using information relating to health or race, or the implementation of a new IT system for storing and accessing Personal Data; and

9.2.2 In carrying out a PIA, Link will include a description of the processing activity, its purpose, an assessment of the need for the processing, a summary of the risks identified and the measures that it will take to reduce those risks, and details of any security measures that require to be taken to protect the personal data

9.2.3 Link is required to consult the ICO in the event that a PIA identifies a high level of risk which cannot be reduced.

10. ARCHIVING, RETENTION AND DESTRUCTION OF DATA

10.1 Link will not store and retain Personal Data indefinitely. It will ensure that Personal Data is only retained for the period necessary. Link will ensure that all Personal Data is archived and destroyed in accordance with the periods specified within the group-wide Data Retention Schedule.

11. MONITORING OF THE POLICY

Any matter which demonstrates a serious failure of internal controls should be reported immediately to the Chief Executive.

12. COMPLAINTS AND APPEALS

Link welcomes complaints and positive feedback, both of which provide information which helps us to improve our services.

If you have a complaint or concern about the way in which Link processes your personal or sensitive data you can make a complaint to:

Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF

0303 123 1113

https://ico.org.uk/concerns/handling/

13. POLICY AVAILABILITY

A summary of this policy can be made available in a number of other languages and other formats on request.

14. POLICY REVIEW

Link undertakes to review this policy regularly, at least every three years, with regard to:

- Applicable legislation, rules, regulations and guidance
- Changes in the organisation
- Continued best practice

Privacy Impact Assessment Screening Questions

Carrying out a Privacy Impact Assessment [PIA] will be useful to any project – large or small – that:

- Involves personal or sensitive data about individuals
- May affect our customers' reasonable expectations relating to privacy
- Involves information that may be used to identify or target individuals

Please tick the applicable statement(s) below. Will your project involve:

1. A substantial change to an existing policy, process or system that involves personal information ☐ Yes ☑ No
2. A new collection of personal information ☐ Yes ☑ No
3. A new way of collecting personal information (for example collecting it online) ☐ Yes ☑ No
4. A change in the way personal information is stored or secured ☐ Yes ☑ No
5. A change to how sensitive information is managed ☐ Yes ☑ No
6. Transferring personal information outside the EEA or using a third-party contractor ☐ Yes ☑ No
7. A decision to keep personal information for longer than you have previously ☐ Yes ☑ No
8. A new use or disclosure of personal information you already hold ☐ Yes ☑ No
9. A change of policy that results in people having less access to information you hold about them ☐ Yes ☑ No
10. Surveillance, tracking or monitoring of movements, behaviour or communications ☐ Yes ☑ No
11. Changes to your premises involving private spaces where clients or customers may disclose their personal information (reception areas, for example) ☐ Yes ☑ No

If you have answered 'Yes' to any of these points, please complete a full Privacy Impact Assessment. If you have answered 'No', you need take no further action in completing a Privacy Impact Assessment.

Equality Impact Assessment Screening Questions

Will the implementation of this policy have an impact on any of the following protected characteristics?

1. Age	☐ Yes	☑ No
2. Disability	☐ Yes	☑ No
3. Gender reassignment	☐ Yes	☑ No
4. Marriage and Civil Partnership	☐ Yes	☑ No
5. Pregnancy and Maternity	☐ Yes	☑ No
6. Race	☐ Yes	☑ No
7. Religion or belief	☐ Yes	☑ No
8. Sex	☐ Yes	☐ No
9. Sexual orientation	☐ Yes	☐ No

If you have answered 'Yes' to any of these points, please complete a full Equality Impact Assessment. If you have answered 'No', you need take no further action in completing an Equality Impact Assessment.