Intra Group Policy

Data Protection Policy

Approval date – July 2021
Review date – July 2024
Version – 2.0

This policy applies to;

Link Group ☒ **Link Housing** ☒ **LinkLiving** ☒ **PSL** ☒

Link Property ☒ **Horizon** ☒ **Larkfield** ☒ **West Highland** ☒

This policy is subject to Freedom of Information publication scheme and is to be published on the following websites;

Link ☒ **LinkLiving** ☒ **Horizon** ☒ **Larkfield** ☒

West Highland ☒

Policy Summary

This policy reflects the requirements of the UK GDPR and the Data Protection Act 2018.

Equality Impact Assessment

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 Impact Assessment

This policy does not have a direct impact on privacy as sets out Link's approach to the processing and management of personal and special category data.

Policy Owner	**Review Manager**	**Approved By**
Director of Human Resources and Business Support	Information Management Co-ordinator	Business Improvement Team

Revision History		
Date	Version Number	Comments
19 July 2021	1.1	Refresh of policy as per three-year cycle and update content to new policy template
30 July 2021	1.2	Update to section 8 to reflect contractual reporting arrangements
30 July 2021	2.0	Policy approved by the Business Improvement Team

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. This 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 personal data and special category personal data from a variety of sources.

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 in adherence to the data protection principles (below) and in a why which demonstrates accountability:

- Lawfulness, fairness and transparency
- Purpose limitation
- Data minimsation
- Accuracy
- Storage limitation
- Integrity and confidentiality (security)

2. SCOTTISH SOCIAL HOUSING CHARTER (CHARTER), REGULATORY AND LEGAL CONTEXT

The following Charter outcomes, regulatory requirements or legislation relates to this policy:

- the UK General Data Protection Regulation [UK GDPR]
- the Data Protection Act 2018
- the Privacy and Electronic Communications (EC Directive) Regulations 2013 (as may be amended by the proposed Regulation on Privacy and Electronic Communications)
- 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.
- Scottish Social Housing Charter, Governance and Financial Management Standard 2 – the RSL is open and accountable for what it does.

The policy will achieve compliance, mitigate and monitor associated risk of non-compliance as follows:

3. ROLES AND RESPONSIBILITIES

3.1 In line with the Information Governance Framework, the following governing boards, leadership teams and individuals have specific responsibilities under this policy:

The **Link Group Board** [LGB] is ultimately responsible, and accountable, for legal and regulatory compliance.

The **Group Leadership Team** [GLT] is accountable for ensuring that the business areas within their areas of operation are compliant with legal and regulatory requirements.

The **Information Governance Board** [IGB] is accountable for developing, and monitoring progress against the Information Management Strategy. The IGB, working within their agreed remit will carry out assurance activities to ensure compliance with legal and regulatory requirements and report compliance to the GLT and the LGB.

An I**nformation Asset Owner** [IAO] is the applicable operational business lead who is accountable for information assets within their business areas. They are expected to understand how information is held, used, and shared and address the risks to the information. They can delegate responsibility for specific assets, or related tasks, to managers, but not the accountability.

The **Senior Information Risk Owner** [SIRO] is accountable for ensuring that Link's approach to information risk is effective.

The **Chief Information Security Officer** [CISO] is accountable for the shaping and implementation of secure processes and systems, in line with legislative and regulatory requirements and driving cyber security initiatives.

The **Data Protection Officer** will monitor compliance with data protection legislation, produce group-wide harmonised operational procedures, and provide advice and guidance on data protection obligations.

All **line managers** are accountable for ensuring their team members are aware of the information governance policies and procedures in place, ensure that mandatory training is completed and promote awareness-raising communications.

All **colleagues** are expected to complete mandatory training, read awareness-raising communications, make themselves aware of the content of information governance policies and take any action expected to comply with these policies.

4. DATA

4.1 All Link data is valuable and must be protected.

4.2 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 group's privacy notices.

4.2.1 "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.

4.2.2 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 "special category personal data".

4.2.3 Link, as per the Code of Conduct, expects colleagues to always respect confidentiality. Failure to do so may be considered an act of gross misconduct which, following a disciplinary investigation, may result in summary dismissal.

5. PROCESSING OF PERSONAL DATA

5.1 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

5.2 Privacy Notices

5.2.1 Link has produced privacy notices which it is required to provide to all data subjects whose personal data is processed by the organisation. That privacy notice will be provided prior to processing their personal data and they will be advised of the terms of the privacy notice when it is provided to them.

5.3 Employees

5.3.1 Employees' personal data and, where applicable, special category 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.

5.4 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.

5.5 Processing of Sensitive Personal Data

In the event that Link processes special category 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.

6. DATA SHARING

6.1 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.

6.2 Data Sharing

6.2.1 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.

6.2.2 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.

6.3 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.

6.3.1 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.

6.3.2 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.

6.3.3 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.

7. DATA STORAGE AND SECURITY

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

7.1 Paper Storage

Link's preference is that data is not stored in hard copy, however, 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.

7.2 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 and managed in line with the Records Management Policy.

8. BREACHES

8.1 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 8.3 below.

8.2 Any identified, or suspected, data breach must be reported to datamanagement@linkhaltd.co.uk immediately. A data breach risk assessment will be carried out to determine whether the breach is likely to result in a risk to the rights and freedoms of the individuals(s), in line with the data breach risk assessment procedure.

8.3 Where Link is operating as a data processor under a commercial contact with external authorities any breaches must be immediately reported to the applicable contract manager to report to the contracting authority, who will act as data controller, in line with the contract obligations.

8.4 Serious data incidents

In the event of high-risk data breach or data incident Link 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, Security Incident Response 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

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

Link is required to report any breaches which are likely to result in a risk to 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.

9. DATA SUBJECT RIGHTS

9.1 Data subjects are entitled to view the personal data held about them by Link, where in written or electronic form.

9.2 Data subjects also 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 communicated through the privacy notices.

9.3 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:

9.3.1 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. Responses to subject access requests will be made through a commonly used electronic format, where possible.

9.3.2 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.

9.3.3 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.

9.4 Right to be Forgotten

9.4.1 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.

9.4.2 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.

9.5 The Right to Restrict or Object to Processing

9.5.1 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.

9.5.2 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.

10. DATA PROTECTION IMPACT ASSESSMENTS (DPIAs)

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

10.2 Link shall:

10.2.1 Carry out a DPIA, in line with the data protection impact assessment procedure 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

10.2.2 In carrying out a DPIA, 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

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

11. ARCHIVING, RETENTION AND DESTRUCTION OF DATA

11.1 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.

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. MONITORING OF THE POLICY

Any matter which demonstrates a serious failure of internal controls should be reported immediately to the Director of Human Resources and Business Support, Group Director of Corporate Services, or the Chief Executive. This policy will be monitored as follows;

- Quarterly reports to the Group Leadership Team and Business Improvement Team
- Six-monthly reports to the Link Group Board
- Internal audit
- The outcome of any investigations carried out by the Information Commissioner's Office

14. POLICY AVAILABILITY

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

15. POLICY REVIEW

Link undertake to review this policy regularly, at least every 3-5 years, with regard to:

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

16. POLICY IMPLEMENTATION CHECKLIST

Policy will be published on Linkipedia and database records updated	☒
Relevant staff teams will be sent a copy of this policy and briefed on key changes	☐
Procedures accompany this policy and are published	☒
If staff training is needed Learning and Development will be contacted	☐
This policy should be sent to staff as a mandatory read	☐

17. DATA PROTECTION IMPACT ASSESSMENT SCREENING

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

A Data Protection Impact Assessment [DPIA] (also known as Privacy Impact Assessment [PIA]) must be completed if the policy involves one or more of the following (please tick each that apply to this policy):

☐ evaluation or scoring;

☐ automated decision-making with significant effects;

☐ systematic monitoring;

☐ processing of sensitive data or data of a highly personal nature;

☐ processing on a large scale;

☐ processing of data concerning vulnerable data subjects;

☐ innovative technological or organisational solutions;

☐ processing that involves preventing data subjects from exercising a right or using a service or contract.

☐ use systematic and extensive profiling or automated decision-making to make significant decisions about people;

☐ process special-category data or criminal-offence data on a large scale;

☐ systematically monitor a publicly accessible place on a large scale;

☐ use innovative technology in combination with any of the criteria in the European guidelines;

☐ use profiling, automated decision-making or special category data to help make decisions on someone's access to a service, opportunity or benefit;

☐ carry out profiling on a large scale;

☐ process biometric or genetic data in combination with any of the criteria in the European guidelines;

☐ combine, compare or match data from multiple sources;

☐ process personal data without providing a privacy notice directly to the individual in combination with any of the criteria in the European guidelines;

☐ process personal data in a way that involves tracking individuals' online or offline location or behaviour, in combination with any of the criteria in the European guidelines;

☐ process children's personal data for profiling or automated decision-making or for marketing purposes, or offer online services directly to them;

☐ process personal data that could result in a risk of physical harm in the event of a security breach.

☐ there is a change to the nature, scope, context or purposes of our processing.

☐ If a DPIA is not carried out, please summarise the reasons below:

This policy, while providing a framework in which personal and special category must be managed, does not itself involve the processing of such data.

18. EQUALITY IMPACT ASSESSMENT SCREENING

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

Age	☐ Yes	☑ No
Disability	☐ Yes	☑ No
Gender reassignment	☐ Yes	☑ No
Marriage and Civil Partnership	☐ Yes	☑ No
Pregnancy and Maternity	☐ Yes	☑ No
Race	☐ Yes	☑ No
Religion or belief	☐ Yes	☑ No
Sex	☐ Yes	☑ No
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.