Data Protection Policy

Approval date – May 2017
Review date – May 2020

This policy applies to

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

Policy Summary

This policy provides a framework for ensuring compliance with the Data Protection Act 1998.

This policy outlines Link's commitment to good information governance and compliance with the eight data protection principles.

Equalities

This policy fully complies with Link's Equality, Diversity and Inclusion Policy.

Privacy

This policy outlines the steps that Link will take to ensure the privacy of customer information. It sets a clear framework to inform customers how their information will be used, how it is shared and how to request a copy of any personal data held on Link systems.

Policy Owner

Director of Finance and Corporate Services

Approved by

Link Group Board

1. INTRODUCTION

This policy has been devised to show how Link Group will deal with legal obligations under Data Protection (DP) legislation and how we will deal with confidentiality.

Data Protection law is designed to give people safeguards to prevent organisations processing personal or sensitive data without the person's knowledge or consent. Personal data is any identifiable data relating to a living individual.

Each active company in the group is required to register individually as a data controller. The public register is held by the Information Commissioner's Office. Registrations are renewed annually.

2. PRINCIPLES

The following principles govern the operation of this policy:

- Processing personal data is a core activity which enables us to provide services. The data protection principles provide a base from which to develop a relationship of trust with people who use our services
- Personal data about individuals will be held and processed in accordance with current DP law
- We will tell our tenants, service users and other customers how we will use their personal data and the circumstances in which we may share it with other organisations
- Sharing of personal data with other organisations will be controlled by the terms of our registration as data controllers, by statutory obligations and by agreements and/ or protocols with partner organisations and other agencies
- All employees and volunteers will treat personal data as confidential and keep it secure
- Personal data of customers, employees and other contacts shall only be accessed and processed electronically using devices checked and issued by the ICT & Digital section of Link Group. This applies equally to telephones, tablets and handheld devices and to laptops and personal computers. Employees will not be permitted to use their own devices for work processes.

3. OBJECTIVES

The objectives of this policy are to ensure that:

- Personal data about individuals is used, stored and shared in accordance with the principles of data protection law
- All tenants, service users and other customers are made aware of how their personal data may be used
- Procedures and systems for information management are implemented to promote the proper handling and security of personal data

4. APPROACH AND METHOD

The Senior Management Group [SMG] in its formal approval of the policy acknowledges that it accepts full responsibility for its implementation. Day-to-day responsibility for the operation of this policy lies with the appropriate directors and managers of the Link group of companies. All relevant employees have a responsibility to ensure that this policy is applied as instructed.

The policy will be implemented using the following approaches:

1. Raising and maintaining awareness of the importance of:

- Treating all personal data entrusted by customers to Link with care and respect
- Explaining clearly to each customer how and why we use personal data, including whether we share it with or make disclosures to other organisations
- Maintaining confidentiality, including carrying out identity or security checks at the start of phone calls, interviews and visits
- Ensuring that evidence of customer consent is recorded where necessary for data processing

2. Keeping paper and electronic notes and records, and the devices on which electronic records are held secure at all times. Electronic processing and storing of personal data must only take place on devices that are issued or approved by our ICT & Digital section for that purpose.

3. Developing systems for:

- Monitoring document and data retention
- Identifying inaccurate data or data which is no longer needed
- Secure deletion and destruction of data

4. CCTV will only be installed and monitored by Link to provide information to assist prevention and detection of crime affecting the safety and security of users of the premises and areas covered. The quality of images will not normally exceed that required for detecting the presence of a person or persons. Sound will not normally be recorded. Employees will not be monitored when carrying out their duties except in situations where their personal safety may be at risk, or when observation is incidental to surveillance described above.

5. Requests from customers and others who provide us with personal data (subject access requests or SARs) will be dealt with promptly and openly. Link will provide access to such information the person is entitled to see, by providing the relevant information either through supply of copies of the original document or where this is not possible or reasonable, providing extracted information on the personal data held. The £10 fee permitted under the Data Protection Act 1998 will not be charged by Link. Data will only be provided to the person who is the subject of the data.

5. MONITORING, PERFORMANCE MEASUREMENT AND REPORTING

Data processing underpins all our services and is the foundation for users of our services to trust Link. Specific reporting on data protection issues should therefore serve to ensure that we have earned that trust and to warn of any incidents which would put that at risk.

Reporting will normally include:

- Incident reporting, e.g. breaches of data security
- Reports on customers' concerns, reflected in SARs and complaints
- Operational reports on systems, summaries of action taken and description of data securely deleted

These areas will be monitored by the appropriate managers within each Link company and/ or function, and reported on regularly to the relevant director. If any significant issues of concern arise these will be dealt with by the director who will report such matter to the appropriate Board. Any matter which demonstrates a serious failure of internal controls should also be reported immediately to the Chief Executive.

These obligations to ensure fair and lawful processing of personal data, particularly keeping each customer's data accurate and up to date, makes it important to review and verify data at every opportunity. All employees accessing personal data records will be made aware of the need to use contacts with customers to review:

- The accuracy of the data
- The length of time the data has been held
- Whether the data is still needed
- Existence of photographic or other images which permit identification of individuals
- Existence and continuing need for sensitive personal data

Procedures will enable employees to take the necessary steps to update or delete data or to alert another person to the need to do so.

Periodic audits of policy compliance will be conducted by the Internal Auditor and/ or the Strategy and Business Support team. Audit results will be reported to the Audit Committee.

6. COMPLAINTS AND APPEALS

Link welcomes complaints and positive feedback, both of which provide information which helps us to improve our services. We use a complaints handling procedure (CHP) developed by the Scottish Public Services Ombudsman (SPSO) and the Scottish Housing Regulator.

The CHP allows for most complaints to be resolved by front line staff within a five day limit (first stage), or if the complaint is complex, a detailed investigation will be made by a manager within a 20 day limit (second stage). At the end of the second stage our response will be made by a director.

At any stage where the customer is dissatisfied, he/ she may refer the matter to the Information Commissioner's Office at www.ico.org.uk/concerns , or write to:
Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF

At each stage Link will advise the customer how the complaint should be taken forward, and advise which agency would be most appropriate to consider the case.

7. POLICY AVAILABILITY

This policy is available on request free of charge from Link. A summary of this policy can be made available in a number of other languages and other formats on request.

2. 8. 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