The Langstane Group

Privacy Policy

Senior management team	19 August 2020
Board / Committee	Board of Management
Approval date	15 February 2021
Implementation date	1 March 2021
Review date	March 2024
Version	V4

Policy Version	Date of Approval	Changes made to Policy
V1	22 June 2009	-
V2	19 February 2016	Full re-write
V3	28 May 2018	Updated in line with General Data Protection Requirements and Scottish Federation of Housing Associations Model Privacy Policy
V4	31 August 2020	As part of review of high level governance policies

1. Introduction and Background

Langstane Housing Association Ltd, and all subsidiary companies comprising the Langstane Group, hereinafter referred to as 'the Association', is committed to ensuring the secure and safe management of data held by the Association. The Association's staff members 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 documentation referred to herein.

Although data protection legislation applies to living individuals, the Association continues to treat data regarding deceased individuals with the principles of data protection in mind.

The Association needs to collect and process certain information about individuals. These individuals include customers (tenants, factored owners etc.), employees and other people the Association with whom has a relationship. The Association manages a significant amount of data, from a variety of sources. This data contains Personal Data and Sensitive Personal Data (known as Special Categories of Personal Data under the General Data Protection Regulation (EU) 2016/679).

Legislation

It is a legal requirement that the Association processes data correctly. The Association must collect, handle and store personal information in accordance with the relevant legislation. The relevant legislation in relation to the processing of data is:

- the General Data Protection Regulation (EU) 2016/679 (the General Data Protection Regulations);
- the Privacy and Electronic Communications (EC Directive) Regulations 2003 (as may be amended by the proposed Regulation on Privacy and Electronic Communications); and
- any legislation that, in respect of 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 European Union.

Principles of Data Protection

The Data Controller (see section 5) is responsible for and shall be able to demonstrate compliance with the principles set out in the General Data Protection Regulations that personal data shall be:

1) processed lawfully, fairly and in a transparent manner
2) collected for specified, explicit and legitimate purposes and not further processed in a manner not compatible with those purposes

3) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed
4) accurate and kept up to date; where necessary taking every reasonable step to have it rectified or erased where it is found to be inaccurate
5) kept no longer than is necessary in a form that allows identification of a Data Subject; personal data may be stored for longer for statistical or research purposes provided there are adequate security measures in place
6) processed in a manner that ensures appropriate security, including safeguarding against breach.

Definitions of Personal Data

For the purpose of this policy the following definitions will apply:

Personal data means data that relates to a living individual (Data Subjects) who can be identified:

- from that data; or
- from that data and other information which is in the possession of, or is likely to come into the possession of, the Data Controller; and
- includes any expression of opinion about the individual and any indication of the intentions of the Data Controller or any other person in respect of the individual.

Special Category Data, previously described as sensitive data, is any sort of data that is held that can be used to identify an individual's:

- racial or ethnic origin,
- political opinions, and trade union membership,
- religious or philosophical beliefs,
- biometric or genetic data,
- physical or mental health or condition,
- sexual life, or sexual orientation.

The Association has procedures for ensuring that all special category data is held and processed in accordance with the General Data Protection Regulations. If the Association wishes to hold or use special category data it must obtain explicit consent from the Data Subject, except where the information is required to comply with Employment Law or to establish or defend legal claims. These conditions are in line with Article 9 of the General Data Protection Regulations.

2. Policy Statement

The Association has clear structures and processes in place to ensure and demonstrate compliance with the General Data Protection Regulations, and all staff members are aware of their responsibilities within the Data Protection framework.

3. Objectives

The objectives of this policy are to:

- ensure the Association complies with, and is in a position to demonstrate compliance with, the principles of the General Data Protection Regulations and any related legislation;
- provide staff with clear information about their responsibilities regarding Data Protection, and have a range of supporting procedures and paperwork to support delivery of good practice in Data Protection; and
- ensure adequate measures are in place to protect personal information, and to deal effectively with a personal data breach.

4. Links to other policies

This policy is related to a number of Association policies and corporate documents, but in particular to:

- Information Security Policy
- Records Management Policy
- Social Media Policy
- Recruitment Policy
- Freedom of Information Policy.

5. Roles and Responsibilities Data Controller

The Chief Executive is Data Controller in terms of the General Data Protection Regulations. It is the responsibility of the Data Controller to ensure the Association complies with Data Protection law. The Support Services Manager is identified as the central point of contact for Data Protection matters, and is responsible for ensuring the Association has an appropriate and adequate Data Protection Framework in place.

Data Protection Officer (DPO)

A Data Protection Officer is an individual who has an over-arching responsibility and oversight over compliance by the Association with Data Protection laws.

Freedom of Information legislation was extended to cover RSL's with an effective date of 11 November 2019. This included a requirement for all RSL's to employ or to engage a Data Protection Officer (DPO) under the General Data Protection Regulations.

Langstane's current (August 2020) arrangements are as follows:

- The Data Controller is the Chief Executive
- The Data Protection Officer is the Support Services Manager
- The Data Protection Officer's name and contact details are contained within the Fair Processing Notice.

The DPO is responsible for:

- monitoring the Association's compliance with Data Protection laws and this policy;
- co-operating with, and serving as, the Association's contact for discussions with the Information Commissioner's Office;
- reporting breaches or suspected breaches to the ICO and Data Subjects.

Departmental Directors

Departmental Directors have responsibility for identifying, recording and reviewing any personal data held by their department, both in paper and electronic form. It is their responsibility to verify information to ensure it is accurate and not held beyond a reasonable length of time. A full schedule of the personal data held in each department, and indicative timescales for data and document retention, is held centrally. This is a live document and is updated and approved by the Departmental Director on at least an annual basis.

Directors are responsible for ensuring their teams are aware of their duties in relation to Data Protection.

Central Point of Contact

The central point of contact for matters relating to Data Protection is the Support Services Manager. Responsibilities include:

- Internal training where requested by the Departmental Directors, or Human Resources section;
- Production of internal paperwork and procedures that are complaint with the General Data Protection Regulations;
- Named responsibilities within various procedures including the Subject Access and Breach Procedures;
- Liaison with appointed staff in each team acting as a 'data protection buddy' to ensure that team processes and practice are compliant with the General Data Protection Regulations; and
- Any other relevant duties delegated by the Data Controller.

Employees

All staff are Data Processors, and are responsible for following the Privacy Policy and associated procedures set out by the Association. The Association provides regular Data Protection training to ensure staff have appropriate knowledge and skills to adhere to the principles of good data protection practice.

Contractors

Contractors are Data Sub-Processors of specific, controlled parts of the Association's personal data. These Data Sub Processors must comply with Data Protection laws. The Association will ensure that, as part of any tendering exercise, all contractors have a binding contract to ensure that robust technical arrangements, policies and procedures are in place for meeting the General Data Protection Regulations requirements.

This will include information relating to subject access requests, data retention and disposal, and a protocol for reporting breaches back to the Association.

These Data Protection responsibilities are clearly set out in the Principle Contract or by an Addendum to the Principle Contract.

6. Processing of Personal Data – the lawful basis

The Association is permitted to process the personal data of Data Subjects provided it is doing so on the following grounds:

- Processing is necessary for the performance of a contract between the Association and the Data Subject or for entering in to a contract with the Data Subject
- Processing is necessary for the Association's compliance with a legal obligation
- Processing is necessary for the purposes of legitimate interests – note that this condition is not available to public bodies as defined in the relevant legislation
- Processing is necessary for the establishment, exercise or defense of legal claims
- Processing is necessary for carrying out obligations or exercising rights related to employment or social security.

The above conditions are in line with Articles 6 and 9 of the General Data Protection Regulations.

7. Fair Processing Notice

The Fair Processing Notice (FPN) or privacy notice is published by the Association on the Association's website, and is available to all individuals whose personal data is held by the Association. The FPN must be available at the outset of processing, and an individual should be advised of the terms when it is provided to them.

A separate FPN is provided to all employees of the Association, and those applying for a vacant post. The Association can process certain types of special category information in order to comply with Employment Law.

In line with Article 13 of the General Data Protection Regulations, the FPN sets out the data that is processed by the Association, and the legal basis for that processing. It informs the Data Subject of their Rights, and who to contact to complain about Data Protection. Full copies of the FPNs are found at Appendix 1 to this policy.

8. Consent to Process Special Category Information

Consent for processing will require to be used from time to time by the Association. It is used where there is no alternative second ground for processing available. Where consent is sought, this is done so in writing. The consent provided by the Data Subject must be freely given, and for a specific and defined purpose. The Data Subject must also be informed that the consent to process the information can be withdrawn.

Individuals are asked to provide their consent for processing Special Category information, used for specific purposes clearly stated by the Association. This includes, but is not limited to:

- Employee consent for medical and equalities monitoring information not explicitly covered by employment law
- Housing applicant consent for processing evidence for medical / harassment / pregnancy priority points on the housing list
- New tenant consent for health-related information, and equalities monitoring information.

9. Image Consent

The Association publishes images on the website, on social media, in leaflets and in other publications such as the Annual Report. Any photograph of a tenant, customer, contractor, or staff member requires consent from the Data Subject. This is recorded separately, and stored centrally until such time as permission to use the image is withdrawn by the Data Subject or, in the case of staff consent for internal photographs, when the employment contract comes to an end.

As with all consent under the General Data Protection Regulations, consent to use the image can be withdrawn. This means that no publication published after consent is withdrawn will contain that image, and the Association website and social media platforms will be updated where it is practical to do so.

10. Data Storage

All data held by the Association will be stored securely, whether in paper or electronically. The Association has an I.T. Security policy in place to ensure there are robust measures in place to protect personal data that is in electronic format.

All departments have a document management protocol in place. This describes where the personal information in the department is stored, how it is kept secure, and how the information is disposed of in order to adhere to the document retention schedule. Each department has a member of staff identified as a 'data protection buddy'. This staff member works with the Support Services Manager to ensure that team data protection practice follows procedure, and the document management protocol is up to date and adhered to.

It is the responsibility of all staff to ensure that personal data is kept secure during their day-to-day duties. Staff are trained to have awareness of good practice in personal data handling to reduce the risk of personal data breaches.

All hard copy personal information is disposed of via confidential waste bins provided at each office location.

Langstane will ensure that all of its policies and practices accord with the following requirements:

Paper Storage

Manual records that contain sensitive / personal information are securely stored at all times.

When system users remove documentation that contains sensitive / personal information, care is taken to protect this from unauthorized access or loss or theft (e.g. it is not left in an area that can be viewed / removed by members of the public).

When the Personal Data is no longer required it will be disposed of by the employee so as to ensure its destruction, excepting certain designated data such as personnel records – which will be destroyed where appropriate by senior managers acting for the employer. 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 the Association's storage provisions.

Electronic Storage, Transfer and Disposal of Data

Information on policy and practices required for the storage, transfer or disposal of electronic data, is contained in Langstane's Information Security Policy

11. Data Retention Schedule

The data retention schedule determines the time period beyond which personal data will no longer be retained. The Data Controller and the appropriate Departmental Directors are responsible for ensuring that data held beyond the time limits set out in the retention schedule is confidentially and satisfactorily destroyed according to internal administrative procedures.

Information about data retention is available on the Association's website, or will be made available upon request by a Data Subject.

12. Disposal of Personal data

The Association cannot store and retain personal data indefinitely. All personal data will be disposed of securely. Paper copies containing any personal data are disposed of using secure confidential waste bins, which are then removed and disposed of appropriately.

Electronically held data that is no longer necessary is checked on a regular basis, and archived or deleted according to the data retention procedure.

Officers working off site will be instructed on any additional measures deemed necessary to reduce the risk of data breach whilst handling personal data.

13. Training

The Association recognises that all staff will be required to handle relevant data at some stage during the course of their employment and they therefore are regarded as Data Processors within the meaning of the General Data Protection Regulations.

The Association provides a comprehensive training plan to ensure everyone concerned understands the implications of the General Data Protection Regulations and the scope of this Policy and, in particular, understands the responsibilities placed on them in the processing of data.

The Human Resources Section is responsible for the identification and implementation of training for staff, including periodic refresher training to ensure all staff have an understanding of their data protection responsibilities.

14. Security

In accordance with the principles of Data Protection, staff are authorised to access and use data only so far as it is appropriate for their jobs or for their understanding of the Association's general policies. Any data, whether manual or electronic, will have access restricted on that basis. System access for all team members is authorised by the Director of each department via the appropriate form identified within the IT Policy.

For much of the data held by the Association, it is appropriate for all staff to have access. Some commercial or sensitive personal information will have restrictions, the breach of which will be a disciplinary matter.

IT have a system for ensuring that all portable storage devices, including mobile phones and laptops, have an appropriate level of security in place to avoid inadvertent breaches or inappropriate access, including password protection when not in use. Data is not held on any Association laptop as all data is accessed via remote connection to the Association's network.

Encrypted USB sticks are in use by staff that require portable data, and for the implementation of the Disaster Recovery Plan.

Identified staff have access to a secure email site for sharing of sensitive data in relation to anti-social behaviour or the monitoring of serious offenders.

15. Data Sharing

From time to time it may be necessary for the Association to share data it has gathered with third parties. Individual departments will have in place clear protocols to ensure that any information shared complies with good practice in Data Protection. As part of ongoing training staff are aware of any information sharing protocol and will follow such protocols when dealing with any sharing requests.

Information Sharing Protocols are a formal document, signed by all parties to the agreement. Where there is no protocol in place, Service Managers will ensure that they consider the following key questions:

1) Does the information enable a living person to be identified? The General Data Protection Regulations do not apply in the case where an individual is deceased. However, information is still to be handled with sensitivity in these cases.
2) Is there a clear and legitimate purpose for sharing information? If not, information will not be shared.

3) Is there consent to share? If not, sharing will proceed only if the organisation requesting the information has a legal right to it.
4) Is the information sharing covered in the privacy notice?
5) Is the information being shared appropriately and securely?
6) Has the decision made about the sharing request been properly recorded?

Once Service Managers have considered all of these points, and are comfortable that it is appropriate to share the information, they should proceed. If there are any doubts about whether sharing data is appropriate, this is discussed with the central point of contact for data protection, or the Data Controller. If it is likely that sharing will occur on a regular basis, then consideration should be given to creating a more formal Information Sharing Protocol.

In any situation where personal information is to be disclosed on a bulk basis rather than for an individual case, this must be checked and approved by the Data Controller according to internal procedures, prior to being released to any third party.

A third party is any person, group or organisation that wishes access to data that is not the subject or authorised to process personal data for the Data Controller.

16. Breach of Data Protection

The Association has reporting duties in the event of the unauthorised disclosure, deletion, alteration, or loss of personal data.

In the event of a breach, an employee will immediately inform the relevant line manager, and steps will be taken to contain the breach as soon as possible by whatever means available. The breach will be reported to the Support Services Manager using the paperwork provided in the breach procedure.
This will be shared with the Data Controller. The Data Controller, will review the case, and judge if it is necessary to inform the Information Commissioner. The Data Controller will also consider whether the breach is notifiable to any third parties in accordance with the terms of any applicable data sharing agreements.

Any breach that is notifiable to the Information Commissioner's Office must be reported within 72 hours of the Association becoming aware of the breach. A notifiable breach is one that significantly impacts on the rights and freedoms of Data Subjects. Whenever a Data Subject's personal information is disclosed in error, the Data Controller will also consider whether it is appropriate to report the breach to the Data Subject as soon as possible in order to protect their rights and freedoms.

Details of any breaches, and the subsequent action taken, will form part of an annual report to the Audit Committee.

17. Subject Access Requests

Data Subjects have the right to obtain a copy of their data held by the Association upon making a request to do so (a Subject Access Request). Upon receipt of a request by a Data Subject, the Association will respond to the Subject Access Request within thirty (30) days of the date of confirming the identity of the person making the request.

The Association will 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; or where the Association does not hold the personal data sought by the data subject. In the latter two situations, the data subject will be informed of the situation.

Staff will follow procedure to ensure timescales are adhered to. Where the personal data comprises data relating to other data subjects, Langstane will take reasonable steps to obtain consent, or where consent cannot be obtained, redact data from third party data subjects, as regards disclosure of that personal data to the data subject who has made the Subject Access Request. All Subject Access Requests go through an approvals process prior to information being released to the Data Subject. This is to protect the Association from the risk of a data breach occurring.

Employees of the Association have the right to ask for a copy of their personal data. This is available upon written request to the Human Resources and Corporate Services Manager. The thirty (30) day timescale also applies under these circumstances.

18. The Right to be Forgotten

A Data Subject can exercise their Right to be Forgotten. This is done by the Data Subject writing to the Association, seeking that the Association erase the Data Subject's Personal Data in its entirety, or they can request a partial erasure of data.

Each request received by the Association 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. The Data Controller will have responsibility for accepting or refusing the Data Subject's request. All such requests will be responded to in writing within thirty (30) days of the request.

Where an individual has enacted their Right to be Forgotten, the letter of request will be retained until the standard period of data retention has elapsed, and the records would have been disposed of within the routine retention system.

19. The Right to Restrict or Object to Processing

A Data Subject may ask that the Association 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 from time to time by the Association, a data subject has an absolute right to object to processing of this nature by the Association, and if the Association receives a written request to cease processing for this purpose, then it must do so immediately. Each request received by the Association will require to be considered on its own merits and legal advice will be obtained in relation to such requests from time to time. The Data Controller will have responsibility for accepting or refusing the Data Subject's request, and will respond in writing within 30 days of the request being received.

20. CCTV

The Association's use of CCTV will not interfere with an individual's right to privacy. In accordance with the General Data Protection Regulations, CCTV is only used in accordance with the purpose for which the system was installed.

All images gathered by the system are written over after 30 days, except in situations where it has been requested as evidence, either as part of an on- going investigation in line with its original purpose, or by law enforcement agencies. In instances where this information is shared, it shall only be held beyond 30 days for as long as it is necessary for the prescribed purpose.

In line with Scottish Government and Information Commissioner's Office Guidance, CCTV systems are reviewed annually by the team responsible for the implementation and monitoring of the system, to ensure they continue to comply with the General Data Protection Regulations.

All data collected is subject to the same right of access as any other personal data held by the Association.

All sites where CCTV is in use have clear signage indicating the purpose of the installation and details of how to contact the Data Controller.

An agreed form is used to determine the basis for the installation of CCTV, and for annual reviews. Review is the responsibility of the Officer responsible for the implementation and operation of the system. This officer is named on the form.

21. Privacy Impact Assessments (PIAs)

Privacy Impact Assessments are a means of assisting the Association in identifying and reducing the risks that operations have on the rights and freedoms of Data Subjects.

In line with Article 35 of the General Data Protection Regulations, the Association will:

- 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
- In carrying out a PIA, 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.

The Association will require to consult with the ICO in the event that a PIA identifies a high level of risk which cannot be reduced. The Data Controller will be responsible for such reporting, and where a high level of risk is identified by those carrying out the PIA they require to notify the Data Controller within five (5) working days.

22. Monitoring and Review

The Directors of individual departments are responsible for the management and maintenance of records of the data they hold. They will manage their staff to update the central point of contact as to any changes to their processes. They will also manage their staff to review their personal data management on at least an annual basis to ensure compliance with the General Data Protection Regulations. Data will be retained or destroyed in line with Langstane's Data Retention Schedule.

The Data Controller will produce and submit an annual report to the Audit Committee that includes assurance on data protection compliance. This will provide:

- The number of subject access requests
- Details of any breaches, and the subsequent action taken,
- The number of requests for deletion, and the subsequent action taken
- Details of any training provided throughout the relevant period.

The Policy will be reviewed at least every 3 years, or following significant changes in legislation.

Right to Complain

In the event you are not satisfied with the service you have received, please contact the Association for a copy of the Complaints Policy, which can also be viewed on the Association's website – www.langstane-ha.co.uk

Equality and Diversity

The Association is committed to promoting equality and diversity across all areas of its work, and discrimination or harassment of any kind is not tolerated.

If you would like this document sent to you in large print, please contact Support Services on 01224 423000.