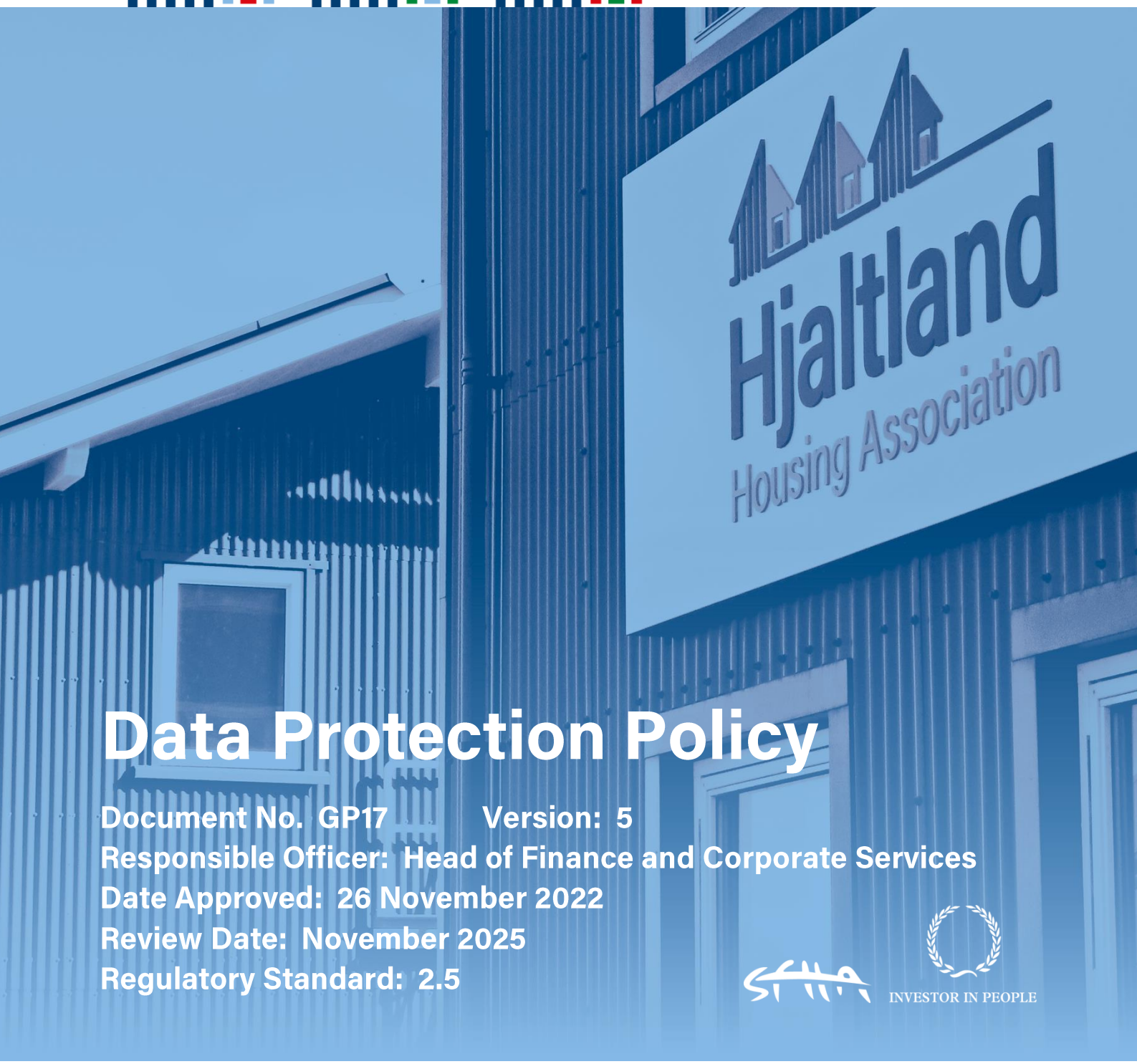
Hjaltland
Housing Association



Data Protection Policy

Document No. GP17 Version: 5
Responsible Officer: Head of Finance and Corporate Services
Date Approved: 26 November 2022
Review Date: November 2025
Regulatory Standard: 2.5

INVESTOR IN PEOPLE

Providing homes, supporting communities

Contents

Hjaltland Housing Association 6 North Ness Business Park, Lerwick, Shetland, ZE1 0LZ
Telephone 01595 694986 | Email mail@hjaltland.org | **www.hjaltland.org.uk**

7.0 Media to be used in Publicity/Promotional Material

1.0 Introduction to the Data Protection Legislation

Hjaltland Housing Association Limited (Hjaltland) is obliged to comply with the terms of the UK General Data Protection Regulation (UK GDPR), tailored by the Data Protection Act 2018. (Together referred to in this policy as the "Data Protection Legislation") The Data Protection Legislation establishes a framework of rights and duties which are designed to safeguard personal data. This framework balances the legitimate needs of an organisation to collect and use personal data for business and other purposes against the right of individuals to respect for the privacy of their personal details.

The Data Protection Legislation is underpinned by a set of data protection principles with the legal duty for enforcing compliance with the Data Protection Legislation falling to the Information Commissioner's Office (the ICO).

Hjaltland is committed to protecting the rights and privacy of individuals in accordance with the Data Protection Legislation.

Personal data is defined as information relating to an identified or identifiable living individual and can be held in any format, electronic (including websites and emails), paper-based, photographic etc. from which the individual's information can be readily extracted.

In order for Hjaltland to operate effectively they have to collect, and process personal data about a range of people including, but not limited to, the following:

- tenants and their relatives / household members;
- staff (past and current members of staff and applicants);
- housing applicants;
- sharing owners;
- factored property owners;
- one stop shop clients;
- Governing Body and Tenant Committee members; and
- contractors/suppliers.

In order for the Hjaltland to comply with the Data Protection Legislation, personal data must be collected and used fairly, stored safely/securely and not disclosed to any third party unlawfully.

All processing of personal data (includes collection, holding, retention, destruction and use of personal data) is governed by the Data Protection Legislation. The Data Protection Legislation applies to all

personal data - whether held on a computer or similar automatic system or whether held as part of a structured manual filing system.

The Data Protection Legislation also covers the transferring of personal data to a third party that is located in a country or territory outside the European Union (EU) this is on the basis of an interim arrangement for the time being.

Failure to comply with the Data Protection Legislation could result in the prosecution not only of Hjaltland but also of the individual responsible for the breach.

Data subjects (that is persons about whom personal data is held) may also sue for compensation for damage and any associated distress suffered where their rights have been infringed as a result of Hjaltland breaching the Data Protection Legislation.

Financial penalties can be imposed on Hjaltland by the ICO for any serious breaches of the Data Protection Legislation. **The maximum financial penalty that the ICO can impose is a fine of £17.5m or 4% of turnover (whichever is greater).**

Given the financial consequences of any serious breach of the Data Protection Legislation, it is imperative that Hjaltland staff, Governing Body Members or contractors concerned with, or having access to, personal data ensure that such personal data is processed according to the principles of data protection and the rights of data subjects.

Staff, Governing Body members and contractors must treat all personal data carefully and must not disclose any personal data to unauthorised persons (this includes parents or relatives of tenants or other data subjects).

Hjaltland is registered with the ICO as a controller as required by the Data Protection Legislation.

Hjaltland's Registration No is: **Z5931029.**

2.0 Policy Scope

This policy applies to:

- all Hjaltland staff;
- all Governing Body members;
- contractors and suppliers appointed by Hjaltland; and
- any bodies or organisations working with Hjaltland in a partnership/joint-working arrangement.

3.0 Equal Opportunities

The Association is committed to promoting positive measures that eliminate all forms of unlawful or unfair discrimination on the grounds of age, disability, gender reassignment, marriage & civil partnership, pregnancy & maternity, race, religion or belief, sex, sexual orientation. Our aim as landlord, service provider and employer is to recognise the needs of all individuals, and ensure these commitments are evident throughout every aspect of our business and our activities.

The Association assesses and reviews all new and revised policies and procedures, we do not see this policy as having any direct impact upon the protected characteristics contained within the Equality Act.

4.0 Data Protection Principles

When processing personal data, Hjaltland will ensure that it complies at all times with the requirements of the Data Protection Legislation. This compliance will ensure all personal data that is collected is processed fairly and for lawful purposes. This personal data will also be stored safely and not disclosed to any other person unlawfully.

In order to achieve the requirements set out in Section 1 of this policy, Hjaltland will comply in full with the data protection principles contained in the Data Protection Legislation in the following terms:

i. personal data should be processed lawfully, fairly and in a transparent manner;
ii. personal data should be obtained for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;
iii. personal data shall be adequate, relevant and limited to what is necessary for the purposes for which it was obtained;
iv. personal data shall be accurate and where necessary kept up to date;
v. personal data is not kept in a form that identifies individuals for longer than is necessary for its purposes; and
vi. appropriate technical and organisational measures shall be taken to protect the security of the data against unauthorised/unlawful processing, loss, destruction, damage to the data.

5.0 Responsibilities for Compliance

Hjaltland is the controller under the Data Protection Legislation. However, the following groups/individuals also have responsibilities for data protection compliance:

- Governing Body members;

- Chief Executive and all departmental/area directors;
- all those in managerial or supervisory roles are responsible for developing and encouraging good information handling practice within their respective departments; and
- staff who process personal information as part of their duties.

The Chief Executive has overall responsibility for data protection matters and for reporting any serious data protection breaches to the ICO and to any affected individuals if required.

The Head of Finance & Corporate Services is responsible for ensuring the required fees have been paid to the ICO and that Hjaltland maintains accurate and up to date records of our data processing activities.

6.0 The Rights of the Individual/Data Subject

Individuals/Data Subjects have the following rights in relation to the processing of their personal data:

- the right to receive information in relation to Hjaltland's processing of their personal data in a "privacy notice";
- the right of access to a copy of the information comprising their personal data;
- the right to object to processing of their personal data in certain circumstances, for example, for direct marketing;
- the right to restrict the processing of their personal data for certain purposes;
- the right to claim compensation for damages caused by a breach of the Data Protection Legislation;
- the right in certain circumstances to have inaccurate personal data rectified;
- the right to request that their personal data is deleted in certain circumstances;
- the right to request their personal data in a particular format for their own use; and
- the right to request the ICO to assess whether any provision of the Data Protection Legislation has been contravened by Hjaltland.

A definition of terms relating to data subjects, and examples of the types of personal data that Hjaltland may collect are listed in Appendix A of this policy.

7.0 Privacy Notices

Before Hjaltland processes an individual's personal data, the individual must be given a "privacy notice" that provides information on how Hjaltland will use their personal data. Privacy notices should be included anywhere we request personal data from an individual, including on forms.

Privacy notices need to include:

- identity and contact details for Hjaltland;

- the purposes and legal basis for processing their personal data – if Hjaltland is processing their personal data for legitimate purposes, details of what those are need to be included;
- details of any recipients of their personal data, including details of any transfers outwith the EU and what safeguards are in place for those transfers;
- details of how long Hjaltland will keep their personal data;
- details of each of the individual's rights in relation to their personal data, including the right to complain to the ICO; and
- if their personal data is required under a contract or statute, details of the consequences of the individual failing to provide their personal data.

If Hjaltland receives an individual's personal data from a third party, then the individual must be given a privacy notice with the details above and details of the types of personal data processed by Hjaltland and where the personal data came from. If Hjaltland knows that the individual already has the privacy notice information or it would involved a disproportionate effort to provide the individual with a privacy notice then it need not provide one. Any decision not to provide a privacy notice must be authorised by the Chief Executive.

8.0 Consent

Where Hjaltland asks an individual for consent to process their personal data, the individual must be sign or submit a consent statement that includes the privacy notice wording and details of what they are consenting to, including different options for them to choose from where possible, and how they withdraw their consent.

The Data Protection Legislation states that it is not always appropriate to ask an individual for consent and consent may be invalid where:

- Hjaltland would process the personal data even if consent is refused by relying on another legal basis under the Data Protection Legislation;
- the consent is asked for as a precondition to a service – for example, a tenant is asked for consent when signing a tenancy agreement; or
- there is an "imbalance of power" between Hjaltland and the individual – for example, an employer / employee or the landlord / tenant relationship.

Hjaltland understands "consent" to mean that the data subject has been fully informed of the intended processing and has signified their agreement, whilst being in a fit state of mind to do so and without pressure being exerted upon them.

Consent obtained under duress or on the basis of misleading information will not be a valid basis for processing. There must be some active communication between the parties such as signing a form and the individual must sign the form freely of their own accord. Consent cannot be inferred from non-

response to a communication. For special category personal data, explicit written consent of data subjects must be obtained unless an alternative legal basis for processing exists.

9.0 Disclosure of Data

This policy determines that personal data may be legitimately disclosed where one of the following conditions applies:

- the individual has given their consent (e.g. an individual has consented to Hjaltland corresponding with a named third party);
- where the disclosure is in the legitimate interests of Hjaltland (e.g. disclosure to staff - personal data can be disclosed to other staff members if it is clear that those staff members require the personal data to enable them to perform their jobs);
- where Hjaltland is legally obliged to disclose the personal data (e.g. Statutory Agencies, Health and Safety returns, ethnic minority and disability monitoring);
- where disclosure of the personal data is required for the performance of a contract with the data subject; and
- where disclosure of the personal data is necessary for Hjaltland to exercise its public functions and powers or perform a specific task in the public interest that is set out in law.

Hjaltland has a statutory obligation to provide certain types of personal data to third party organisations such as the Police, local authorities and the Department of Work and Pensions. In cases such as this, there is no requirement to gain consent from the data subject prior to disclosing the requested personal data. However, where there is no statutory obligation to disclose personal data to a third party, then explicit consent will be sought by Hjaltland from the Data Subject/individual, unless there is a more appropriate legal basis under the Data Protection Legislation.

The Data Protection Legislation permits certain disclosures without consent so long as the information is requested for one or more of the purposes listed below. This type of information disclosure will only be accommodated providing the requests are supported by the appropriate legal documentation:

- to 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);
- to prevent serious harm to a third party; and
- to protect the vital interests of the individual, this refers to life and death situations.

10.0 Data Subject Rights

In accordance with the Data Protection Legislation, all individuals or their authorised representatives have the right to access any personal data, which are held by Hjaltland in electronic format and structured manual/paper record.

These information requests are referred in the Data Protection Legislation as 'Subject Access Requests' (SAR). Individuals or authorised representatives who submit requests to Hjaltland will be provided all the relevant information to which they are entitled by law subject to any statutory exemptions.

Any individual who wishes to exercise this right to submit a request should apply in writing to the Data Protection Officer (DPO). Hjaltland reserves the right to charge a fee for repetitive or excessive requests in accordance with the Data Protection Legislation. This right will only apply in exceptional circumstances and any such request should be complied with within one month of receipt by Hjaltland of the written request, regardless of whether a fee is required.

Where it is not possible to meet the one-month time limit due to the request being manifestly unfounded or excessive, particular in the case of repetitive requests, Hjaltland may extend the time limit in exceptional circumstances by two months, provided we inform the individual of the extension within one month.

All staff requests will be directed to their line manager. The line manager will then inform the DPO of the request by the staff member.

11.0 Retention & Disposal of Data

The Data Protection Legislation does not set out any specific minimum or maximum period for retaining personal data. Instead, the Data Protection Legislation states personal data processed for any purpose shall not be kept longer than is necessary by Hjaltland.

It is therefore necessary to consider the reasons for collecting personal data and if the personal data should be retained when the relationship between Hjaltland and the individual ends, i.e. former tenants or staff members.

Tenants

In general, electronic tenant records containing information about individual tenants are kept 6 years following the end of their tenancy as per the retention period unless any debt is left outstanding, information would then be kept indefinitely to allow reinstatement of the debt if another application is made and information would typically include name and address, date of entry and date of exit.

Departments should regularly review the personal files of individual tenants in accordance with Hjaltland's Document Retention and Destruction Guidance in Appendix B.

Staff

In general, electronic staff records containing information about individual members of staff are kept for 6 years following the end of their employment as per the retention schedule (there are however some exceptions which are noted separately in the retention schedule), information would typically include name and address, positions held, leaving salary. Other information relating to individual members of staff will be kept according to the Document Retention and Destruction Guidance in Appendix B.

Information relating to unsuccessful applicants in connection with recruitment to a post must be kept for 12 months from the interview date. Hjaltland may keep a record of names of individuals that have applied for, be short-listed, or interviewed, for posts indefinitely. This is to aid management of the recruitment process.

Hjaltland will ensure at all times that personal data is disposed of in a way that protects the rights and privacy of data subjects. Typical methods employed by Hjaltland for disposal of data including the following:

- shredding;
- disposal as confidential waste; and
- secure electronic deletion of data files.

12.0 Special Categories of Personal Data

As required under the Data Protection Act 2018, Hjaltland has assessed its purposes for processing of special categories of personal data and shall ensure compliance with the data protection principles as follows:

i. Lawfulness, fairness and transparency – Hjaltland has undertaken a data audit and maintains a record of its processing of special categories of personal data, which includes an assessment on the legal basis and special condition under which such data is processed. Hjaltland is satisfied that we have a legal basis and special condition for holding the relevant special categories of personal data, which is referred to within Hjaltland's privacy notices;

ii. Purpose limitation – Hjaltland's purposes for collecting special categories of personal data are specified within Hjaltland's privacy notices;

iii. Data minimisation – Hjaltland has accessed the datasets held and has guidance in place to ensure that only the special categories of personal data which are necessary for our purposes are held;

iv. Accuracy – Hjaltland will continually check for accuracy and take steps to correct any inaccuracies, should they arise;

v. Storage limitation – Hjaltland has a document retention policy and has assessed appropriate retention periods for special categories of personal data; and

vi. Integrity and confidentiality – Hjaltland has procedures in place to ensure the security of special categories of personal data and will have additional security measures for such data, where appropriate.

13.0 Data Security

There is a duty placed on Hjaltland by the Data Protection Legislation to ensure there is appropriate security to prevent personal data being accidentally or deliberately compromised.

All staff, Governing Body members and appointed contractors are responsible for ensuring that any personal data which they hold is kept securely and not disclosed to unauthorised third parties. Only authorised staff, Governing Body members and appointed contractors can access, alter, disclose or destroy personal data within the scope of their authority.

Personnel files will be stored in locked cabinets, and access to computerised records will be password protected. Staff should also ensure any personal data displayed on a PC screen cannot be viewed by an unauthorised third party either in the workplace or when using any form of digital media device in a public place.

In terms of minimising risks associated with breaches of the Data Protection Legislation through lapses in personal IT security, staff with access to personal data should always ensure their PC is 'locked' if they need to leave their desk.

Any misuse of personal data or breaches of data security by staff, Governing Body members or contractors may result in disciplinary or legal action being taken against the individual.

14.0 Breaches

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

Internal Reporting

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

- As soon as it becomes known the breach or potential breach has occurred, and in any event no later than six (6) hours after it has occurred, the Association's Corporate

Services Officer (CSO) or DPO must be notified in writing of (i) the breach; (ii) how it occurred; and (iii) what the likely impact of that breach is on any data subject(s);
- The Association must seek to contain the breach by whichever means available;
- The breach must be logged on the Data Breach Register
- The DPO or CSO must consider whether the breach is one which requires to be reported to the ICO and to the Data Subjects affected and, if appropriate, will do so in accordance with this clause 7;
- Notify third parties in accordance with the terms of any applicable Data Sharing Agreements.

Reporting to the ICO
The DPO will require to report any breaches which pose a risk to the rights and freedoms of the Data Subjects who are subject of the breach to the Information Commissioner's Office ("ICO") within 72 hours of the breach occurring. The DPO must also consider whether it is appropriate to notify those Data Subjects affected by the breach.

15.0 Risk Management and Audit

Hjaltland aims to mitigate the risk of potential financial penalties and compensation payments through failure to adhere to the Data Protection Legislation through the provision of training to staff on data protection issues as detailed in Section 12 of this policy. Hjaltland will also review this policy and the associated procedures on a regular basis to ensure that they meet all legislative and regulatory requirements and best practice guidance. In addition, a review of the personal data held by Hjaltland will be carried out as part of the Internal Audit plan to ensure ongoing compliance with the provisions of the Data Protection Legislation.

Internal audit procedures will form an important part of establishing and sustaining good data protection practices. Hjaltland will review the personal data it processes and collects and assess this against the data protection principles as listed in Section 4 of this policy. This will inform the review of our action plan to ensure compliance with this policy.

Hjaltland undertake self-assessment to periodically check our compliance with the Data Protection Legislation; our Data Protection Policy and guidance, regulatory and good practice guidance; our registration with the ICO; our working practices in the collection, processing and storage of personal data and achievement of our Action Plan.

Data protection issues will be considered as part of the Risk Management Strategy, and if assessed as a priority risk area the commitment of resources will be considered to attend to the controls to mitigate these risks.

16.0 Training

All individuals permitted to access personal data in line with their work duties will be trained in data protection following the implementation of this Data Protection Policy and Guidance. All individuals with access to personal data on or behalf of Hjaltland, individuals must agree to undertake any relevant training that may be deemed appropriate.

Data protection training will form part of the Induction training of new staff members. A copy of this Data Protection Policy and Guidance will be provided to all staff members (including Agency Staff) and Governing Body members.

17.0 Policy Review

Date approved by Management Committee: 21/11/2019

This policy will be reviewed in November 2025 and thereafter every three years although *ad hoc* changes may be made to the policy during the three-year period if any the following occur:

- responding to any new legislative changes in the Data Protection Legislation; and
- to address any weaknesses in the policy that has been identified by Hjaltland as a result of a breach in data security.

1. Appendices

More detailed guidance on the following issues has been published by the Association:

A. Definition of Terms
B. Document Retention and Destruction Guidance
C. Procedure for Subject Access Requests (SAR)
D. Management of Tenant Records
E. Disclosure of Tenant Information
F. Staff Records Management
G. Media to be used in Publicity/Promotional Material

Hjaltland Housing Association 6 North Ness Business Park, Lerwick, Shetland, ZE1 0LZ
Telephone 01595 694986 | Email mail@hjaltland.org | **www.hjaltland.org.uk**

Appendix A

Definition of Terms

Data Subject

This refers to any living individual who is the subject of personal data – i.e. the individual who can be identified from that data. Examples of data subjects for Hjaltland are:

- tenants and their relatives / household members;
- staff (past and current members of staff and applicants);
- housing applicants;
- sharing owners;
- factored property owners;
- one stop shop clients;
- Governing Body members; and
- contractors/suppliers.

Personal Data

Personal data is data that relates to an identified or identifiable individual. It also includes any expression of opinion or view about an individual or their circumstances.

Examples of personal data include, but not limited to, the following:

- age;
- address;
- housing history;
- economic status; and
- payment information.

Special Categories of Personal Data

The Data Protection Legislation also recognises that some items of data are more sensitive than others and therefore require additional protection to ensure appropriate handling.

Examples of special categories of personal data include, but are not limited, to the following:

- racial or ethnic origin;
- political opinions;
- religious or other beliefs;

- data relating to health (e.g. support services received or medical data);
- genetic or biometric data (where used for identification purposes); and
- data relating to an individual's sex life or sexual orientation.

Processing

The Data Protection Legislation applies to the "processing" of personal data by Hjaltland, which means any operation personal on the personal data, including collecting, storing, using, amending, disclosing or deleting.

Controllers and processors

Hjaltland is the controller of the majority of the personal data that we process. This is because we determined how and why it is processed. Hjaltland also engages "processors" to process personal data on our behalf.

Data protection officer (DPO)

Harper Macleod LLP
The Ca'd'oro
45 Gordon St
Glasgow
G1 3PE

Appendix B

Document Retention and Destruction Guidance

1. Introduction

Storage space costs money. Maintaining an ever-growing set of paper files and archives takes up time and other resources. Even where material is stored on a computer system (e.g. in a document imaging system), such a system will only be of value if it is manageable and accessible. What documents does Hjaltland need to keep and for how long?

It would be impossible to list all the documents Hjaltland keeps, or needs to keep. In many cases, it will be a matter of what 'feels right' for Hjaltland and the exercising of common sense when making a decision on what to keep, what to archive or what to dispose of.

However, you should keep in mind the need to comply with the Data Protection Legislation and specifically the principle that *'personal data should not be kept in a form that identifies individuals for longer than is necessary for its purposes'*.

As a rule the Limitation Act 1980 is followed. This Act in many cases sets a six year time length after an event has occurred for keeping documents. This can be after employment ceases (for employment records and personnel charts) or the resolution date for a whistleblowing event or termination of a contract with suppliers, agents etc.

Hjaltland's Data Retention Schedule lists the principal documentation that we should keep, together with details of statutory retention periods and recommended retention periods.

2. Storage medium

The medium in which documents are stored is electronically by OMNI system and Sage Cloud 50 Payroll system which are both password protected and limited access. Electronic files are also password protected, Hardcopy files are kept under lock and key with limited access.

The medium in which documents are stored is largely a matter for each organisation. However, care should be taken to ensure that documents stored electronically will capture all the information on the document (front and back) and allow the information to be presented in a readable format and if necessary, be readily convertible to a paper format.

HM Customs and Excise has particular requirements relating to electronically stored data, and has the power to withdraw approval for such media in any individual case. It is advisable to obtain legal advice on the admissibility of electronically formatted documents for presentation in a court of law.

Appendix C

Procedure for Data Subject Rights

Individuals wishing to access their personal data should submit a request in accordance with the following notes:

1. Make your request, in writing, to the Data Protection Officer.

2. The request should include details and provide documented evidence of who you are (e.g. driving licence, passport, and birth certificate). You should also provide as much detail as possible regarding the personal data you wish to access (e.g. where and by whom information is believed to be held, specific details of information required etc.).

3. You are not required to state why you wish to access the personal data: the details we require are merely those that will aid the efficient location and retrieval of information containing your personal data.

4. Hjaltland adopts a general policy of openness in terms of allowing individuals access to their personal data. However, Hjaltland reserves the right to charge a fee for manifestly unfounded or excessive, particularly repetitive requests and for additional copies of the personal data (as permitted under the Data Protection Legislation).

5. Once Hjaltland receives a Request, all efforts will be made to fully comply within one month. In any event, you will receive all the personal data that has been located and can be released within one month and an explanation for any personal data that cannot be provided at that time and notification that Hjaltland will extend the time period by up to two months for complex or numerous requests, where appropriate.

6. In accordance with the Data Protection Legislation, Hjaltland does not usually release personal data held about other individuals without their consent. Therefore, if information held about you also contains personal data related to a third party, Hjaltland will make every effort to anonymise the personal data. If this is not possible, and Hjaltland has been unable to secure the relevant consent, Hjaltland may decide not to release the personal data.

Handling Subject Access Requests

These guidance notes cover the procedures for handling "Subject Access Requests" and should be read in conjunction with Hjaltland's Data Protection Policy. This document is Appendix C to that policy.

Section 1: General - What is a Subject Access Request?
Section 2: Responding to "Simple" Requests
Section 3: Responding to "Complex" Requests
Section 4: Third Party Data
Section 5: Records Management
Section 6: Association Position on charging for Subject Access Requests
Section 7: Exemptions

Section 1: General - What is a Subject Access Request?
The Data Protection Legislation gives individuals (data subjects) a number of rights including the right to access personal data that an organisation holds about them. This right of access extends to all personal data held on an individual and includes (but is not limited to) personnel files, tenant record files, databases, interview notes and emails which has the individual as the subject of that information. If an individual makes a request to view their personal data, it is known as a "Subject Access Request".

The Data Protection Legislation stipulates that an individual must:

- make the request in writing;
- supply information to prove who they are (to eliminate risk of unauthorised disclosure); and
- supply appropriate information to help Hjaltland to locate the information they require.

Upon receipt of a request, Hjaltland must provide:

- confirmation that their personal data is being processed;
- a copy of their personal data; and
- information relating to the processing of their personal data by Hjaltland, including:
    - the purposes of the processing;
    - the categories of personal data;
    - any recipients of their personal data or proposed recipients;
    - details of how long their personal data will be kept;
    - details of the individuals' rights under the Data Protection Legislation, including the right to complain to the ICO; and
    - details of who provided their personal data if it was not the individual.

Hjaltland must respond to Subject Access Requests within one month.

For further information, see Hjaltland's procedure to be followed when submitting a Subject Access Request.

Section 2: Responding to "Simple" Requests

Whilst data subjects are entitled to request all the personal data that Hjaltland holds on them, experience shows that they are usually looking for something specific. Therefore, the majority of requests received by Hjaltland are likely to be from staff and tenants asking for copies of a specific document(s). These will usually be located from a single source - typically the tenant files - and will not involve the disclosure of personal data relating to a third party. In such cases, Hjaltland' s policy is to be open and transparent and wherever possible to let the individual have a copy of the information with minimum fuss.

Such requests should be handled directly by the relevant department or section and there should be no need to involve the Chief Executive. When responding to such requests, take care to ensure that you do not inadvertently release third party personal data without their consent.

Section 3: Responding to "Complex" Requests

There may be some instances when a request for personal data is more complex and will need to involve the Chief Executive to ensure a co-ordinated response.

Examples of situations where more complex requests might arise include:

- request involves locating information from multiple sources;
- request involves the release of contentious information;
- request is one in a series of requests from the same individual;
- request involves the release of third party personal data for which consent has been refused or cannot be obtained (see Section 4 for further information); and/or
- the individual does not want to ask for the personal data from the department that holds it.

In such cases, the request should be referred to the Chief Executive who will ensure that a co-ordinated approach is adopted and will determine whether or not it is appropriate to charge a fee under the Data Protection Legislation. When responding to Subject Access Requests, the Chief Executive will liaise with staff in the department/section as appropriate.

Section 4: Third Party Personal Data

It will sometimes be the case that responding to a Subject Access Request will lead to incidental disclosure of details relating to some other third party (for example, a referee or another tenant). Such third party personal data should not be disclosed without first seeking the consent of the third party.

If consent cannot be obtained (e.g. the third party cannot be contacted) or is refused, Hjaltland needs to consider whether or not disclosure is reasonable, taking into account:

- any duty of confidentiality owed to the third party;
- the steps taken to seek consent;
- whether the third party is capable of giving consent; and
- any express refusal of consent.

If you are unable to obtain consent, you are advised to contact the Chief Executive who will have to consider/balance the impact on the third party of the disclosure, and the impact on the data subject of the disclosure being withheld. Where third parties have been acting in an official capacity it may be argued that the duty of confidence is lower than is otherwise the case. However, decisions will be made on a case by case basis.

If the Chief Executive decides that disclosure cannot be made, only that information which could identify the third party should be withheld (e.g. third party details are blanked out). Wherever possible, Hjaltland will follow good practice by explaining to the individual that some information has been withheld, and why.

Third parties who regularly supply information on tenants/staff in a professional capacity should be informed that anything they submit may become available to the data subject through a Subject Access Request. Departments are advised to seek consent to disclose at the collection stage (e.g. when requesting references) to avoid delay upon receipt of a Subject Access Request. Where professionals request that information supplied by them be kept confidential, they must supply details of the exceptional reasons for making the request. Hjaltland will consider those reasons in order to decide whether they are valid. For example, there are exemptions under the Data Protection Legislation for information that constitutes legal advice, which is covered by legal professional privilege.

Section 5: Records Management

The maintenance of appropriate records is extremely important in the event of a Subject Access Request. Knowing who keeps what and where is central to the effective and efficient retrieval of information.

The other important aspect of records management is ensuring that only appropriate information is retained. This will reduce the amount of information which must be disclosed (thereby saving time and administrative costs associating with locating and supplying the information) but will also avoid embarrassment and potential damage to Hjaltland's reputation by ensuring that inappropriate personal data is not being retained on individuals.

All staff are advised:

- to be careful about what personal data they keep (including emails);
- to try to only record factual information;
- where it is necessary to record an opinion about an individual, to make sure it is justified and wherever possible backed up with factual evidence; and
- **NOT** to record anything that they would not wish the individual to see.

There are many long-term aims of rationalising the personal data held by Hjaltland. It will certainly help us to respond effectively to Subject Access Requests. The fewer data sources Hjaltland has, the easier it will be to search these on receipt of a Subject Access Request.

Wherever possible, we should be aiming to manage personal data on a single central database. All staff are encouraged not to hold files on individual tenants or staff members, but to lodge any such information within "designated files". Personal data of departed staff and tenants should be reclaimed from any remote sources and stored in a single location or on a single database, with appropriate security and back-up.

Section 6: Association Position on charging for Subject Access Requests

The Data Protection Legislation permits organisations to charge for responding to manifestly unfounded or excessive, particularly repetitive, Subject Access Requests. Hjaltland will only charge for Subject Access Requests in exceptional circumstances and approval of the Chief Executive should be sought before requesting a fee from an individual. Any fees should be requested as soon as possible, and at least within seven days, of Hjaltland receiving the Subject Access Request.

Section 7: Exemptions

There are certain situations where Hjaltland may not be obliged to release personal data in response to a Subject Access Request.

Examples include:

- data containing personal data relating to a third party for which consent to release the personal data cannot be obtained;
- management forecasts such as plans for redeployment, restructuring, promotions (if they would prejudice conduct of business/activity); or
- information relating to legal proceedings being taken by Hjaltland against an individual, which relates to Hjaltland's negotiations with the individual, which would prejudice Hjaltland's position if released.

Hjaltland Housing Association 6 North Ness Business Park, Lerwick, Shetland, ZE1 0LZ
Telephone 01595 694986 | Email mail@hjaltland.org | **www.hjaltland.org.uk**

Exemptions are an extremely complex part of the Data Protection Legislation and must be treated with caution. If you think that an exemption might apply to a Subject Access Request received by your department, you should contact the Chief Executive in the first instance.

Appendix D

Management of Tenant Records

The Data Protection Legislation gives individuals the right to access the personal data that an organisation holds on them. In order to comply with this part of the Data Protection Legislation,

organisations need to have in place effective means of extracting and retrieving personal data from a variety of sources.

Hjaltland holds a great deal of personal data on our tenants, usually in a variety of forms and locations. In order to comply with a subject access request, Hjaltland will need to be able to locate and collate the personal data quickly. It is therefore vital that key personnel know what information is held and by whom. Ideally, all personal data relating to individual tenants should be kept in the tenant files (paper or electronic) so that, in the event of a subject access request, Hjaltland can be confident that all the personal data is easily accessible from a limited number of central sources. However, Hjaltland recognises that this may not always be the case in practice. Hjaltland should ensure that tenant record files are as complete as possible but it is acknowledged that there may be some instances where designated individuals need to retain personal data on tenants which would not be appropriate for more general access.

Information held on tenants can be categorised in one of two ways:

- "classified information" is information which a tenant has requested be kept confidential between the tenant and the designated individual to whom they disclose the information.); and
- "unclassified information" is all other information held on tenants which will be available for general access by designated individuals.

The following guidelines should be followed:

1. Copies of unclassified information relating to an individual tenant should be lodged in the tenant record file.
2. Designated individuals may retain copies of classified information without copying it to the tenant record file.
3. Designated individuals may retain duplicate copies of any documentation (whether electronic or paper), particularly if the information is consulted on a regular basis.
4. Members of staff, other than those responsible for the tenant record files and designated personnel, should not retain information (electronic or paper) about individual tenants.
5. Information should only be retained in accordance with the suggested retention periods in Hjaltland's Records Retention Schedule.
6. When a designated individual leaves Hjaltland, they should pass all information to the member of staff responsible for house files, to be either destroyed (in accordance with Hjaltland's records retention schedule), or filed in the house record file, or passed to a replacement designated individual.
7. Tenants should be informed of how Hjaltland processes their personal data, including what personal data is being held about them, what it will be used for, where it will be stored, and to whom it might be disclosed in a privacy notice. This will normally be achieved via privacy notices within housing application forms and other data collection forms.

If these guidelines are followed, personal data held on tenants can be easily located from a limited number of sources and departments will be much better prepared to respond to subject access requests efficiently.

Appendix E

Disclosure of Tenant Information

Hjaltland must ensure that personal data held on tenants is not disclosed to unauthorised third parties including family members, friends, and Government bodies and, in certain circumstances, the Police. All staff should exercise caution when asked to disclose personal data held on tenants to third parties.

These guidance notes should be read in conjunction with Hjaltland's Data Protection Policy, which includes a section on Disclosure of Data.

Sections

1. General Information.
2. Disclosure to Work Colleagues.
3. Disclosure to Relatives/Guardians and Friends.
4. Confirmation of Tenant Status
5. Disclosure to Shetland Islands Council.
6. Request for personal references
7. Disclosures to the Police and Legal Proceedings.
8. Audit.
9. Survey/Research Organisations.
10. Forwarding Tenant Correspondence on behalf of a Third Party.

Section 1: General Information

Disclosing Personal Data

In accordance with the Data Protection Legislation, personal data should only be disclosed if there is a lawful basis for the disclosure. We may be required to share personal information with statutory or regulatory authorities and organisations to comply with statutory obligations.

We may also be required to publish personal information to meet the Scottish Housing Regulator's regulatory requirements or our legal obligations under the freedom of information legislation. Hjaltland will only publish your personal information where we believe it is lawful.

The most likely lawful bases applicable to the disclosure of tenant data to third parties are:

- where there is a statutory obligation on Hjaltland (e.g. statistical returns);
- disclosure is required for performance of a contract with the tenant (e.g. a tenancy agreement); or
- perform tasks in the public interest under duties as a Registered Social Landlord.

Disclosing Special Categories of Personal Data

In accordance with the Data Protection Legislation, special categories of personal data should only be disclosed where there is a lawful basis and a condition relating to the processing of special category personal data applies under the Data Protection Legislation. The most likely lawful bases applicable to the disclosure of special categories of tenant data to third parties are:

- the tenant has given their explicit (ideally written) consent;
- disclosure is necessary for health or social care purposes (e.g. to provide social care); or
- disclosure is in the vital interests of the tenant (e.g. information relating to a medical condition may be disclosed in a life or death situation).

Disclosing Personal Data Overseas

The Data Protection Legislation restricts the transfer of personal data by Hjaltland outwith the European Union. This applies to personal data which is disclosed to a third party located outwith the EU or where personal data is transferred to a server which is hosted outwith the EU.

There are specific conditions for international transfers of personal data under the Data Protection Legislation. Hjaltland's policy is not to transfer personal data outwith the EU unless the Chief Executive is satisfied that the conditions under the Data Protection Legislation are met.

Requirement to Disclose?

Unless there is a legal or statutory obligation, you are advised not to disclose any personal data about tenants unless there is a lawful basis for the disclosure and tenants have been informed of the disclosure in a privacy notice. Please note that disclosure includes confirmation of a tenant's residence with Hjaltland. If you are in any doubt as to the legitimacy of a disclosure, then no disclosure should be made.

Method of Disclosure

Disclosures should not be made over the telephone. The minimum security option is to take a number and ring the enquirer back. However, it is strongly advised that all enquirers should be asked to submit their requests in writing (where appropriate on headed paper). Once you have checked whether or not the request is legitimate, you should, wherever possible, reply in writing.

Section 2: Disclosure to Work Colleagues

You should always think carefully before disclosing tenants' personal data to work colleagues whether they are from within, or external to, your own department. Under the Data Protection Legislation, you should not disclose personal data to colleagues unless they have a legitimate interest in the data concerned. As a rule you should consider whether or not the information is necessary to allow your colleague to perform their job.

When sharing information with colleagues, you should consider the level of detail necessary to enable them to perform their job. So for instance, if you knew that a tenant was going to be absent from their accommodation for a significant period of time, you may wish to notify colleagues in the department of this fact. However, it might not be appropriate for all colleagues to be made aware of the specific reasons (health or otherwise) resulting in the absence.

Section 3: Disclosure to Relatives/Guardians and Friends

Hjaltland has no responsibility or obligation to disclose any personal data relating to tenants to relatives, even if they are contributing to the rent or other fees.

All tenants should be given the opportunity, both on their tenancy agreement and housing application form to provide the name of a nominated individual to whom Hjaltland may disclose personal data. You should always check a tenant's record to see whether or not they have identified a nominated individual. You may come under pressure to discuss individual tenants with parents/guardians or even friends. However, in these situations it is essential that you do not disclose personal data without the prior consent of the tenant - it would be a breach of the Data Protection Legislation to do so. If the tenant has identified a nominated individual they should have provided express consent within an appropriate consent statement and privacy notice.

You are free to discuss procedures with parents (e.g. describing allocations procedures, advising on when rent should be paid by, etc.) but the specific circumstances of an individual tenant cannot be discussed without the consent of that tenant.

There may be occasional, exceptional circumstances (in which a tenant's life or health is threatened) in which the usual need to get consent before disclosing to parents/guardians may be waived. Hjaltland holds details of tenants' "next of kin" for such purposes, which are explained to the tenant in the privacy notice within the housing application form.

Section 4: Confirmation of Tenant Status

Tenant status is regarded as personal data and therefore must be processed in accordance with the Data Protection Legislation, this includes protecting the personal data against unauthorised disclosure. By confirming whether or not an individual is (or has been) a tenant of Hjaltland could be a breach of the Data Protection Legislation.

Hjaltland receives enquiries regarding individual tenants' status on a regular basis. The nature of the third party requiring the information can range from future providers of rented housing genuinely trying to confirm details on a housing application form to estranged or abusive partners trying to trace

an individual's whereabouts. Therefore, whenever faced with a request for confirmation of tenant status, you should exercise caution before responding.

The majority of requests will be from agencies with a genuine interest in the information. For this reason, tenants are informed (within a privacy notice on their application form) that, if requested, details of their tenant status will be disclosed to certain named bodies. Tenants are given an opportunity to object to these disclosures and so you should always check the tenant's record before responding. You should always employ appropriate security measures to check the identity of the enquirer and you should not disclose the information over the telephone. Wherever possible, ask the enquirer to put their request in writing, preferably on headed paper.

For other enquirers, where there is no statutory or other legal obligation for you to disclose information, you should not confirm or deny the tenant status of an individual without their consent.

Section 5: Disclosure to Shetland Islands Council (includes Housing Benefit Administration)

Tenants are informed that details of their tenancy may be passed to the Shetland Islands Council on their housing application form and are given an opportunity to object to such disclosures.

Section 6: Requests for Personal References

If you receive a request for a personal reference relating to a tenant, you should ensure that

1. the information contained in the reference is factually correct;
2. where possible, keep the disclosure to a minimum;
3. special category personal data (e.g. details of health) must not be disclosed without the explicit consent of the tenant;
4. where opinions about a person's suitability are disclosed, your comments are defensible and justifiable on reasonable grounds;
5. if you are unable or unwilling to give a reference, such a refusal is communicated carefully, without, in effect, implying a negative reference and thus disclosing personal data; and
6. you do not disclose any information if asked to give an unsolicited reference (for a tenant who has not, to your knowledge, cited your name as a referee).

The identity of the person requesting the reference should always be confirmed prior to disclosure. Requests for references should usually be made in writing on headed paper. If you receive an email request for a reference, you should be assured that it is a valid request and is from a known source or company domain. You should process the request but you may wish to reply in written format to a known postal address for the company/organisation.

Telephone references are not usually recommended. However, they are acceptable if the Tenant has specifically asked you to provide a reference at short notice. As a minimum security measure it is recommended to ring the enquirer back to check that they are who they claim to be.

Tenants are informed, within the privacy notice and the application form and mutual exchanges that we will confirm tenant status to future housing providers, provided a mandate from the new housing provider is received and signed by the tenant. Tenants are, of course, given the opportunity to object to this and if they do so, it will be recorded on their tenant record. The Tenant Handbook also informs tenants that we archive tenant records after termination of the tenancy, in order to confirm requests from future housing providers, to provide references etc.

If a tenant cites your name as a referee, Hjaltland's privacy notice should inform the tenant that you will disclose their personal data in this situation unless they object. If you are not aware that a tenant has cited you as a referee, you should check the validity of the request.

Section 7: Disclosures to the Police and Legal Proceedings

Disclosures to the Police

Disclosures to the Police are not compulsory except in cases where Hjaltland is served with a Court Order requiring information. However, the Data Protection Legislation does allow limited exemptions meaning that Hjaltland may release information to the Police in limited circumstances. Such disclosures should only be made if the Police confirm that they wish to contact a named individual about a specific criminal investigation and where Hjaltland believes that failure to release the information would prejudice the investigation. Staff must not release information to the Police over the telephone. The Police must inform Hjaltland in writing. Most Police forces will have their own request form which should always include a statement confirming that the information requested is required for the purposes covered in the exemption, a brief outline of the nature of the investigation, the tenant's role in that investigation, and the signature of the investigating officer.

Legal Proceedings

The Data Protection Legislation exempts data from certain provisions (e.g. informing the tenant or subject access requests) in cases where disclosure is necessary "for the purpose of, or in connection with, legal proceedings or for the purpose of obtaining legal advice, or is otherwise necessary for the purposes of establishing, exercising or defending legal rights". In practice this means that Hjaltland can disclose information regarding tenants to its own solicitors when seeking proper legal advice about a case. However, for cases that do not directly involve Hjaltland, information should only be disclosed if Hjaltland considers it appropriate to apply the exemption. If the information is vital to a case, a Court Order may be issued demanding the information.

Section 8: Audit

Like all other housing associations, Hjaltland appoints external and internal auditors who will see some tenants' personal data during the course of their investigations. Tenants are made aware of this possibility within a privacy notice given in conjunction with the tenancy agreement / housing application form.

Section 9: Survey/Research Organisations

Survey/Research organisations may approach you for a list of addresses or emails for tenant so that they can market their services or circulate a survey. You must not release this information but instead can offer to mail the information/survey on their behalf. If you do decide to undertake a host mailing, you should include a statement explaining the context of the mailing and reassuring tenants that their personal data have not been released to the third party

Section 10: Forwarding Tenant Correspondence on behalf of a Third Party

You should not release tenant addresses or contact details to a third party without the consent of the tenant. Instead you may offer to forward correspondence to a tenant on behalf of a third party. Sometimes you may even receive unsolicited correspondence with a request to forward it to a tenant. You must take care when handling such requests. Remember that an individual's tenant status is personal data. Therefore, if you receive such a request it is important to neither confirm nor deny that that person is a tenant of Hjaltland.

Hjaltland Housing Association 6 North Ness Business Park, Lerwick, Shetland, ZE1 0LZ
Telephone 01595 694986 | Email mail@hjaltland.org | **www.hjaltland.org.uk**

Appendix F

Management of Staff Records

The Data Protection Legislation gives individuals the right to access the personal data that an organisation holds on them by making a subject access request.

Hjaltland holds a great deal of information on its staff. In order to comply with a subject access request, Hjaltland will need to be able to locate and collate the personal data quickly. All information relating to individual staff members should be kept in the staff record files (paper or electronic) so that, in the event of a subject access request, Hjaltland can be confident that all the personal data is easily accessible from a limited number of sources.

The following guidelines should be followed:

1. Wherever possible, copies of documentation relating to an individual member of staff should be lodged in the staff record file(s) (paper or electronic).
2. Designated individuals are permitted to retain duplicate copies of any documentation (electronic or paper), particularly if the information is consulted on a regular basis.
3. Exceptionally, designated individuals may also keep documentation relating to sensitive information (e.g. relating to health or other problems) without copying the information to the staff record file. Designated individuals should only follow this practice when unauthorised access/disclosure of the information concerned to other staff poses a risk of damage/distress to the member of staff.
4. Staff, other than those responsible for the staff record files and designated personnel, should not retain information (electronic or paper) about individual members of staff.
5. The exception to this is email as it would be impractical for staff to pass all emails to a central source. However, all staff must be aware that in the event of a subject access request, they may be asked to search their email archives for all emails referring to the member of staff that has made the request. Therefore, staff are advised not to keep emails relating to other members of staff unless it is absolutely necessary. In writing emails referring to other members of staff, you are reminded that, in the event of a subject access request, that member of staff is entitled to receive copies of all emails which refer to them.
6. Information should only be retained in accordance with the suggested retention periods in Hjaltland's Records Retention Schedule.
7. Staff should be informed of what information is being held about them, what it will be used for, to whom it might be disclosed and whether or not it will stored staff record file.

If these guidelines are followed, personal data held on staff can be easily located from a limited number of sources and Hjaltland will be much better prepared to respond to subject access requests efficiently.

Appendix G

Media to be used in Publicity Material

These guidance notes cover the use of photographs in various media/publicity documents and should be read in conjunction with Hjaltland's Data Protection Policy.

General Photographs
If individuals are not readily identifiable from the photograph and it seems unlikely that any damage or distress will result from such processing then it will not be necessary to obtain consent. Therefore, tenants and staff whose images appear as incidental detail in publicity photographs will not need to give consent for the use of their image.

Photographs of Group Activities
Where photographs are to be taken of a group activity (e.g. a seminar) then this should be announced in advance so that individuals may leave the room briefly if they do not wish to appear in the photographs.

Photographs of Small Groups/Individuals
Where photographs are to be taken of a single individual, or a small group of individuals, where individuals are the main subject of the photograph (even if they are not identified by name), consent should be sought before any photographs are taken. When gaining consent, it is important to ensure that individuals are informed of what the images will be used for (e.g. where they will be printed and who will have access to them) within a privacy notice as part of the consent statement.

Publishing Photographs on the Web
Publishing photographs on the Internet potentially transfers personal data outside of the EU for which rules on gaining consent from individuals are much stricter. If photographs (except where tenant/staff images appear as incidental detail) are to be published on the Internet, written consent should be obtained from the subject(s). Hjaltland will make reasonable efforts to ensure that such consent has been obtained before use and where this is not possible will avoid use where it may reasonably be considered likely to cause the data subject damage or distress. Hjaltland will also respond promptly to any subsequent request to remove a photograph from the web site by an individual who is clearly identifiable in that image.