# DATA PROTECTION POLICY & PROCEDURES

| | |
|---|---|
| Prepared By | Maureen McDonald-Cooke, Policy Officer |
| Policy Created | May 2018 |
| Date of Last Review | N/A |
| Date of Current Review | January 2020 |
| Date of Next Review | January 2023 |
| Reviewed By | Maureen McDonald-Cooke |

| **CORPORATE FIT** | |
|---|---|
| Internal Management Plan | □ |
| Risk Register | □ |
| Business Plan | □ |
| Regulatory Standards | □ |
| Equalities Strategy | □ |
| Legislation | □ |

**contents**

**Appendices 1 to 4 contain procedural information**

## 1.Introduction

Part of our key strategic aims of The Albyn Group is to build our values into our policy and decision making on a daily basis. With that in mind, we aim to follow our current values, which can be located here: https://www.albynhousing.org.uk/about-us/

1.1 The Albyn Group Data Protection Policy is intended to provide a framework for the Albyn Group and all subsidiaries (the 'Group') on ensuring compliance with the General Data Protection Regulation ("GDPR") 2016/679 Data Protection Act 2018
("the 2018 Act").

1.2 The Group needs to collect information about people with whom it deals in order to carry out its business and provide its services. Such people include tenants and their families, service users, employees (present, past, and prospective), Board and Committee members, suppliers, partners and other business contracts, and members of the public.

1.3 This Policy shall apply across the Group and is intended to ensure a standardised approach throughout the Group to our data protection responsibilities.

## 2. Scope

This Policy covers the Group. All employees (whether permanent or temporary) including those that are mobile working and working off site or working within joint partnerships, agency workers, contractors, consultants, modern apprentices, secondees, work experience placements and volunteers shall comply with this Policy and must be aware of what they must do to protect the security of information.

## 3. Aims and Objectives

3.1 Good information governance and data protection compliance are an integral part of our day-to-day work. The Group holds a wide range of personal information and special categories of personal data. We have a duty to protect this information and ensure it is not seen or accessed by people (whether internal or external to the Group) without the authority to do so.

3.2 The key aims of this Policy are to:

- Set out a framework for information governance compliance;
- Identify the business activities of the group which impact upon privacy through the use of data protection impact assessments;
- Provide regular training on this policy and related procedures to raise awareness and ensure compliance with this policy; and
- Reduce the opportunity for security breaches.

3.3 Any failure to comply with the Policy may breach confidentiality and will expose the Group to potential breach of customer, stakeholder, partner and/or supplier trust. A breach of this policy may also result in or contribute to theft of intellectual property, fraud and /or identity theft. Furthermore, failure could constitute a breach of our legislative, regulatory and /or contractual requirements including of our statutory obligations under Data Protection Legislation, which could also result in a fine and /or court action against the Group.

## 4. Organisational Benefits

4.1 There are benefits to embedding compliance with the Data Protection Principles into our culture and Group. These include:

- Protecting the rights and interests of individuals (such as tenants and their families, our service users and staff) whose personal information we hold;
- Supporting good governance;
- Promoting business efficiency and underpinning service delivery;
- Supporting compliance with other legislation and regulations which requires personal information be processed in accordance with the data protection principles;
- Improving accountability and enabling compliance with the data protection legislation and other rules and requirements to be demonstrated;
- Protecting the rights and interests of stakeholders;
- Protecting the group's reputation and brand image; and
- Protecting the Group's assets.

**5. Roles and Responsibilities**

5.1 Whilst responsibility for the implementation of this Policy rests with our Board and Leadership Team, it is incumbent upon everyone to whom this policy applies, including managers, teams and employees to embrace and adhere to data protection "good practice" at all times.

5.2 The **Group Chief Executive Officer** has ultimate responsibility for compliance with the Data Protection Legislation and for enforcing compliance in relation to this Policy.

5.3 **Directors and members of the Leadership Team** have overall responsibility for compliance with the Data Protection Principles within their business division and each business division within the Group should have a nominated member of staff with specific day to day responsibility for data protection compliance within that division. However, it is nonetheless incumbent upon **all teams and employees** to:

- Achieve and demonstrate an adequate level of general awareness of information security and confidentiality;
- Familiarise themselves with and adhere to the key procedures, practices and guidance; and
- Participate actively in information security and exercises when required.

5.4 All **Board and Committee Members** who, during the course of their duties, deal with personal information must comply with this Policy.

5.5 The **Company Secretary** has particular responsibility for maintenance and implementation of this Policy in order to ensure that the Group complies with its legal and regulatory duties. The Company Secretary will report as necessary to the Group Board.

5.6 The **Data Protection Officer** can provide advice and guidance in conjunction with our legal support package on legal requirements of information governance and data protection compliance.

5.7 it is a standard condition of our contracts that our agents and sub-contractors will comply with the Data Protection Legislation, particularly where they are processing personal information on the Group's behalf.

**6. The Data Protection Principles**

6.1 These are the principles with which the Group must by law, comply with when processing personal information, including when the Group is collecting, holding, using and destroying personal information. These principles are set out in Appendix 1.

## 7. Authorised of sharing of Information

7.1 In certain circumstances (and subject strictly to conditions set out in the Data Protection Legislation) personal information may be shared by the Group with other organisations and partners.

7.2 Personal Information may be shared systematically, for example, by way of the routine sharing of information for an agreed purpose or purposes. Where this occurs, this must be underpinned by adherence to strict conditions and procedures to be governed by a Data Sharing Agreement.

7.3 The Group is subject to the terms of the Freedom of Information (Scotland) Act 2002 ("FOISA") and the Environmental Information (Scotland Regulations 2004 ("the EIR's).

These provide individuals with the right of access to any information held by the Group. Where a request is made under FOISA or the EIRs for personal information, this may be disclosed if the disclosure would not contravene any of the Data Protection Principles.

7.4 The Group is fully committed to the aims of FOISA and the EIRs, and will make every effort to meet its obligations. Information will only be withheld where FOISA or EIRs expressly permits it.

7.5 For more information, please see the Group FOI Policy which can be found on our staff Intranet (hyperlink) and or our website. A hard copy is also available on request.

Customers may also request a copy of the policy in other formats and community languages.

7.6 The Group may decide, or be asked, to share personal information in situations which are not covered by a Data Sharing Agreement. In some cases, this might involve a decision about sharing in "one-off" circumstances such as an emergency.

7.7 The Group is regularly requested to disclose personal information to other public sector organisations and by law firms in connection with legal proceedings. Such requests should be passed to the Data Protection Officer who will consider the following:

If the requester has authority to request the information, for example, if a mandate is required:

- If there are any applicable exemptions;
- What privacy notice information has been provided to the individual in question and if this is sufficient to cover the proposed disclosure in compliance with the first data protection principle; and
- If the disclosure would breach any of the Data Protection Principles.

7.8 Before the Group can share personal information it must consider all of the legal implications of doing so, not simply the terms of the Data Protection Legislation. The Authorised Sharing of Information Guidance can be found at Appendix 2

## 8. Data Breach

8.1 Sometimes a breach of information/data security may occur because personal information has been:

- Accidently disclosed to an unauthorised person or persons;
- Lost, for example, through human error or due to fire or flood or other damage to the premises at which it was held;
- Stolen, for example, as a result of a targeted attack (such as a break-in or via cyber-attack) or theft; or
- Otherwise misused.

8.2 Security incident management is a process of handling security incidents in a structured and controlled way. To achieve this, it is essential that breach management plans are put in place to set out how any personal data breach will be dealt with.

8.3 It is for each individual area of the business to develop their own plan to enable any personal breach occurring within that business area to be effectively managed. The Data Protection Breach Management Guidance can be found at Appendix 3. The Data Protection Officer will be responsible for determining whether a breach requires to be reported to the Information Commissioner's Office.

**9. Accountability**

9.1 The Data Protection Legislation includes an accountability principle, which requires the Group to demonstrate that we comply with the Data Protection Principles, as part of this, the Group has implemented this Policy and will put procedures in place to ensure that records of our Processing activities are maintained in accordance with the Data Protection Legislation.

9.2 The records of our Processing activities will comprise of:

- Name and details of the Group, including details of all subsidiaries and our Data protection Officer;
- A description of the categories of individuals, personal information and recipients of personal information;
- Details of transfers to third countries, including documentation of transfer mechanism safeguards in place;
- Retention schedules; and
- A description of technical and organisational security measures.

9.3 The Group also undertakes data protection impact assessments for proposed new projects in line with Data Protection Legislation requirements and has a template form and guidance for completion.

**10. Individual's rights**

10.1 The individual whose personal information we process have the following rights under the Data Protection Legislation:

- The right to be informed;
- The right to rectification;
- The right to erasure;

- The right to restrict processing;
- The right to data portability; and
- The right to object.

10.2 Individuals also have rights in relation to automated decision-making and profiling – i.e. where a system takes decisions without human intervention.

10.3 Details of the procedures for complying with these rights are set out in Appendix 4.

## 11. Key terms

**"consent"** means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which they, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to them.

**"controller"** means the organisation that determines the purposes and means for processing personal data.

**"Data Protection Principles"** means the data protection principles under the GDPR as set out in Appendix 1.

**"personal information"** means any personal data that relates to and identifies (either directly or indirectly) an individual from information which is held by the Group. It also includes any expression of opinion or view about an individual or their circumstances. Examples of personal data relating to individuals includes their:

- name;
- age;
- date of birth;
- contact details;
- marital status;
- housing history;
- financial status; and
- allowance, benefits and grants claimed.

**"personal data breach"** means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed, eg accidental loss, destruction, theft, corruption or unauthorised disclosure of personal data.

**"Processing**" means any activity that involves the use of personal data, including: obtaining; recording; holding; organising; amending; retrieving; using; disclosing; erasing; or destroying personal data.

**"special categories of personal data"** means personal data which the GDPR says are more sensitive, and so needs more protection. This includes data relating to:

- Race or ethnic origin;
- Political opinions;
- Religious or other beliefs of a similar nature;
- Physical or mental health or condition;
- Trade union membership;
- Sexual life or sexual orientation; or

- Genetic or biometric data where processed for the purpose of uniquely identifying an individual.

## 12. Equal Opportunities Statement

12.1 This Policy complies with fully with the Group's Equal Opportunities Policy. We recognise our pro-active role in valuing and promoting diversity, fairness, social justice and equality opportunity by adopting and promoting fair policies and procedures.

12.2 We are committed to providing fair and equal treatment for all our stakeholders including tenants and will not discriminate against anyone on the grounds of race, colour, ethnic or natural origin, language, religious belief, age, sex, sexual orientation, gender re-alignment, disability, marital status, pregnancy or maternity. Indeed, we will positively endeavour to achieve fair outcomes for all.

12.3 We carry out Equality Impact assessments when we review our policies. We check polices and associated procedures regularly for their equal opportunity implications. We take appropriate action to address inequalities likely to result or resulting from the implementation of our policies and procedures.

## 13. Legal and Regulatory Framework

13.1 We adopt and regularly review best practice and in data protection and information governance. The Group aims to operate in accordance with best practice principles for information security and governance such as may be in place from time to time.
This includes (but not limited to): Data Protection Act 2018;

- General Data Protection Regulations (EU) 2016/679;
- Regulation on Privacy and Electronic Communications 2017/0003;
- Human Rights Act 1998;
- Freedom of Information (Scotland) Act 2002;
- Regulation of Investigatory Powers (Scotland) Act 2000;
- Crime and Disorder Act 1998;
- Environmental Information (Scotland) Regulations 2004;
- Management of Offenders etc. (Scotland) Act 2005;
- Police Act 1997;
- Serious Organised Crime and Police Act 2005;
- Information Commissioner's Office Data Protection Code: Employment Practices;
- Information Commissioner's Office Data Protection Code: Subject Access Request;
- Information Commissioner's Office Data Code of Practice: Data Sharing
- Information Commissioner's Office Code of Practice: Consent; and
- All other relevant guidance and Codes of Practice published by the Information Commissioner's Office from time to time.

## 14. Performance Monitoring

The Group will put in place a system which monitors and measures performance under this Policy. Regular compliance monitoring will be undertaken through the Group's Audit and Risk Management Committee with updates being disseminated to the Head of Finance and Corporate Services.

## 15. Policy Review

We will review this Policy every three years and upon changes to the Group. More regular reviews will be considered where, for example, there is a need to respond to new

legislation/policy guidance. Reviews will consider legislative, performance standards and good practice changes.

## Appendix 1

## Data Protection Principles

1. The data protection principles provide that personal information shall:

- **Principle 1** – be processed lawfully, fairly and in a transparent manner;
- **Principle 2** – be obtained only for specified , explicit and legitimate purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes;
- **Principle 3** – be adequate, relevant and limited to what is necessary in relation to the purpose for which it is processed;
- **Principle 4** – be accurate and, where necessary, kept up to date;
- **Principle 5** – not to be kept in a form which permits identification of individuals for longer than is necessary for the purpose it is processed; and
- **Principle 6** – be processed in a way to ensure appropriate security of the personal information, including to prevent unauthorised or unlawful Processing and protected against accidental loss, destruction or damage, using appropriate technical or organisational measures.

2. The processing of personal information is integral to the Group's operations. The Group respects the privacy of the individual and regards the lawful processing of personal information as central to the successful operation of its business and delivery of services. The Group routinely processes personal information about its employees, customers, and other individuals; for example, to register customers applications, to recruit, monitor and manage staff, to Process salaries and expenses and to protect health and safety. E.g. via the use of CCTV.

3. "Processing" has a wide definition in terms of the GDPR and encompasses anything at all that can be done to personal information during the entirety of its lifecycle, including destroying and deleting it. Information is a valuable asset to the Group; it is essential that the Group allows the individuals who personal information we Process to be confident that their personal information will be protected from accidental or deliberate loss, damage, or disclosure or from unauthorised alteration or destruction.

4. When processing personal information, the Group will always ensure that it complies with the Data Protection Legislation and any other relevant privacy laws. To comply and used fairly, stored safely and not disclosed to any other person unlawfully. To do this the Group must comply with the six Data Protection Principles which are set out above.

5. The Group is committed to storing and disposing of all personal information in a responsible and secure manner and will therefore hold personal information for the minimum time necessary to fulfil its purpose. Timescales are set out in the Group's retention schedules and in statute. The retention Schedules can be found on the staff intranet site.

## Appendix 2

## Authorised Sharing of Information Guidance

1. In certain circumstances (and subject strictly to conditions set out in the Data Protection Legislation) personal information may be shared by the Group with other organisations and partners. This may occur, for example, by way of:

    - A reciprocal exchange of information;
    - Different parts of the same organisation making information available to each other;
    - One or more organisations providing to a third party or parties;
    - Several organisations pooling information and making it available to each other;
    - Several organisations pooling information and making it available to a third party or parties; or
    - One-off disclosures in unexpected or emergency situations.

2. Personal information may be shared systematically, for example, by way of the routine sharing of information for an agreed purpose or purposes. Where this occurs, this must be underpinned by adherence to strict conditions and procedures. For example, if consent is required from the individual before making their personal information can be shared, by obtaining that consent and by making robust arrangements for the secure transmissions of any information which is to be shared.
3. The Group may decide, or be asked, to share information in situations which are not covered by routine agreement, In some cases this might involve a decision about sharing one-off circumstances. This might include an emergency.
4. Before the Group can share personal information, it must consider all of the legal implications of doing so, not only simply the terms of the Data Protection Legislation. The following questions will assist in deciding whether it is appropriate to share personal information:

**Systematic Sharing**

- Is the sharing justified?
- What is the sharing meant to achieve?
- Have the potential benefits and risks to individuals whose personal information is involved been assessed?
- Is the sharing proportionate to the issue you are addressing?
- Could the objectives be achieved without sharing the personal information?
- Has the information been given to the Group in confidence?
- Is there any requirement for consent to be given before such personal information can be shared (and, if so, is that consent in place)?

**One-off request**

- Is the sharing justified?
- Have the potential benefits and risks to those individual(s) whose information is involved been assessed?

- Are there concerns that the individual(s) whose personal information is involved is at risk of serious harm?
- Has the information been given to the Group in confidence?
- Is there any requirement for consent to be given before such personal information can be shared (and, if so, is that consent in place)?
- Is there any legal obligation to share the personal information?

If the decision is taken to share personal information in these circumstances, key points to additionally consider include:

- Has the identity of the person requesting the information been validated? This is essential.
- Is it clear what personal information has been requested?
- What personal information needs to be shared? Only share what is necessary
- How should the personal information be shared?
- Personal Information must be shared securely.
- Is it appropriate / safe to inform the individual that their personal information has been shared?
- Whether other privacy laws apply?
- Are there any other legal obligations or rules other than the Data Protection Legislation which may apply to the sharing, for example, contractual duties, duties of confidence, industry-specific regulation or copyright?
- How will the parties provide individuals with the personal information they are entitled to regarding the processing for transparency and fairness?

If the decision is taken to share personal information, a Data Sharing Agreement should be put in place to set out the parameters of the agreement and to underpin the arrangements for the sharing, before any personal information is shared within another party. A Data Sharing Agreement should cover:

- What information needs to be shared – detailed datasets;
- The organisations that will be involved;
- The purpose(s) of the information sharing exercise and the period during which the sharing exercise will operate;
- Statement explaining why the sharing is proportionate to the purpose(s);
- Obligations to ensure that the information is accurate and provisions for recording in the same format;
- Measures to ensure adequate security measures are implemented and maintained in order to protect the information;
- Agreed technical and organisational security arrangements for transmission of information;
- What arrangements need to be in place to provide individuals with access to their personal information, and deal with any other requests from individuals and complaints;
- Agreed common retention periods for holding the information;
- Procedures for dealing with breaches;
- Processes to ensure the secure deletion of the information take place; and
- Provisions for reviewing and terminating the agreement.

Once a decision has been made as to whether or not information should be shared, that decision must be recorded, together with the reasoning behind that decision. Where a decision was taken to share the information, an audit trail must be kept to include details of the following:

- What personal information was shared and for what purpose(s);
- Who it was shared with;
- When it is shared;
- The justification for sharing;
- Whether the personal information was shared with or without the consent of the individual; and
- Whether a data sharing agreement was put in place for the sharing exercise (and if not, the reasoning as to why not).

## Transferring personal information outside the EU

When sharing personal information that the Group is the controller of, we must consider whether this will result in any personal information being transferred outside the EU. For example, many cloud-based servers are located within the United States and transferring personal information to an organisation that will store it on a server located in the US will result in a transfer outside the EU.

The Group must also be aware of sharing any personal information to international organisations in order to ensure that the requirements of the GDPR are met.

The Group should only transfer personal information outside the EU or to an international organisation in the following circumstances:

- The European Commission has decided that the country or international organisation ensures an adequate level of protection and issues an "adequate notice" under GDPR;
- If transferring to the US, whether the personal information transfer is covered by the EU-US Privacy Shield framework;
- Where the Group has put in place appropriate safeguards and there are enforceable rights and effective legal remedies for individuals; or
- One of the derogations under the GDPR applies.

Appropriate safeguards will apply where:

- There is a legally binding and enforceable instrument between public authorities or bodies;
- The ICO has approved binding corporate rules under the GDPR;
- The standard data protection clauses as adopted by the European commission or by the ICO and approved by the European commission are put in place; and
- There is an approved code of conduct or certification mechanism in place in accordance with the terms of the GDPR.

The derogations in the GDPR provide that personal data may be transferred outside the EU for certain specific situations where:

- The individual has consented to the transfer;
- The transfer is necessary for the performance of a contract between the group and the individual, including pre-contractual steps requested by the individual, or a contract made in the interests of the individual between the group and another person;
- The transfer is necessary for important reasons of public interest;
- The transfer is necessary to establish, exercise or defend legal claims;
- The transfer is necessary to protect the vital interests of the individual or other persons, where the individual is physically or legally incapable of giving consent; or
- The transfer is made from a register, which under UK or EU law is intended to provide information to the public.

## Appendix 3

### Personal Data Breach Management Guidance

All personal data breach incidents (whether actual or suspected) must be reported immediately to the Data Protection Officer. Breaches of a criminal nature must be immediately notified to the Director of Finance and Corporate Services. Breaches involving electronic data and / or systems involving electronic information and / or systems must also be immediately notified to the ICT.

Security incident management is the process of handling security incidents in a structured and controlled way. To achieve this, it is essential that breach management plans are put in place to set out how any personal data breach will be dealt with.

Each plan must address five core elements:

- Identification and classification;
- Containment and recovery;
- Risk assessment;
- Notification of breach; and
- Evaluation and response.

It is for each individual business area to develop their own plan and procedures based on Group guidance, taking account of these five elements, to enable any personal data breach occurring in that business area to be effectively managed. Each breach and potential breach may be different, so this guidance does not prescribe for every possible incident. Instead, each case will instead turn on its individual circumstances, but all the elements of a plan should be adhered to.

The **five core elements** referred to above are more particularly explained as follows:

**Identification and Classification**

All staff members must be able to identify a security incident, including personal data breaches. This will allow for early recognition of an actual or possible breach and for prompt, appropriate action to be taken.

In this respect staff need to be fully aware as to what might constitute a breach. A personal data breach may take many different forms, these are some examples of security incidents that may lead to personal data breaches:

- Personal information is accidentally disclosed to unauthorised persons;
- Personal information is irretrievably lost, for example, through human error or due to damage resulting from fire, flood or other cause;
- Personal information is stolen, for example as a result of a targeted attack (including cyber-attack) or theft; or
- Personal information is otherwise misused (inclusive of fraud).

Any suspected breach should be classified under one of the above four headings.

Details of the breach should be recorded accurately, including (but not limited to) the date and

time the breach occurred, the date and time it was detected, who reported the breach, description of the breach, details of any ICT systems involved and any corroborating materials such as error messages, log files, etc.

**Containment and Recovery**

All personal data breaches should be contained and investigated. The relevant business area suffering the personal data breach must, carry out an investigation to identify the circumstances of the actual or suspected personal data breach, how the personal data breach can be contained (which involves limiting the scope and impact of the personal data breach) and what steps need to be put in place to recover any personal data information that is no longer within their control and where necessary limit any damage.

If a personal data breach occurs the relevant business division must:

- Establish who in the group needs to be made aware of the personal data breach and inform them of what they are expected to do to assist in this exercise. For example, this might entail notifying ICT to isolate a compromised section of the network, or to change access rights, help find a lost file or piece of equipment;
- Decide on who will take the lead in investigating the personal data breach and ensure that the appropriate resources are made available for the investigation;
- Establish whether there is anything that can be done to recover the losses or limit the damage the personal data breach can cause; and
- Where appropriate inform the police (for example, in the case of incidents which a crime has (or may have) been committed).

**Risk Assessment**

Before deciding what steps are necessary further to an immediate containment, there must be an assessment of the risks which may be associated with the personal data breach. In assessing such risks, the relevant business divisions should consider what the potential adverse consequences for the individual(s) affected by the personal data breach might be i.e. how likely it is that adverse consequences will occur and, in the event of such consequences occurring, how serious or substantial are they likely to be. In assessing the risk, the relevant business area should consider the following:

- What are the risks to the individual's rights and freedoms?
- What type of personal information is involved?
- How sensitive is the personal information? For example, some information is classed as special categories of personal data because of its personal nature (health records) while other data types are sensitive because of what might happen if it is misused (bank account details);
- If the personal information has been lost or stolen, are there any security mechanisms in place? For example, password protection, encryption;
- What has happened to the personal information? For example, if the data has been stolen, could it be used for purposes that are harmful to the individuals to whom they relate?
- What harm can come to the individual(s) affected by the breach? For example, are there risks to physical safety or reputation, discrimination, financial loss or a combination of these and / or any other aspects?
- What could the personal information tell a third party about the individual to whom it

relates? For example, data could mean very little to an opportunistic thief while loss of data to a determined fraudster might allow them to build up a detailed picture of the people whose data they have obtained, allowing them to then commit identity fraud;
- How many individuals are affected by the personal data breach? It is not necessarily the case that greater risk stems from a loss of large amounts of personal information, but it is an important factor in the overall assessment;
- Who are the individuals whose personal information has been breached? For example, staff, customers, service users, contractors, suppliers. This will to some extent determine the level of risk posed by the personal data breach; and
- Are there wider consequences to consider such as loss of customer, public or stakeholder confidence?

**Notification of Personal Data Breach**

Informing the right people of a personal data breach is an important step in the personal data breach management plan. The Data protection Officer is required to notify the Information Commissioner's Office in the event that the risk is likely to result in a risk to the rights and freedoms of individual. Communication of a personal data breach to the individual is only triggered where it is likely to result in a high risk to their rights and freedoms.

- All personal data breach incidents (whether actual or suspected) must be reported to the Data Protection Officer in the first instance. Breaches involving electronic data and / or systems involving electronic information and / or systems must also be notified to the ICT. Immediate internal notification is essential.
- Initial notification as above may be made verbally where the urgency of the situation demands, however, verbal notification must be followed immediately by completion and submission of a Data Breach Report Form.

- Under no circumstances should the business area(s) involved inform the Information Commissioner's Office directly. Any notifications requiring to be made to the Information Commissioner's Office must be dealt with by the Data Protection Officer.
- In certain cases, the Data protection Officer will be required to notify the Information Commissioner's Office within 72 hours of the Group becoming aware of the personal data breach and also possibly the individuals concerned without undue delay, this is why it is vital that personal data breaches are notified to the Data Protection Officer immediately.

The following questions will assist in deciding whether to also notify individuals or other organisations and stakeholders, who may be affected, about the personal data breach:

- Will notification help meet security obligations? For example, will notifying a contractor mean that a gap in security may be closed?
- Can notification help an individual affected by the personal data breach to mitigate any risk? For example, by cancelling a bank card or changing a password;
- Is notification for the particular group / individual affected appropriate? For example, children or vulnerable adults; and
- Are there risks in over-notifying? Not every incident will warrant notification depending on the facts and circumstances of the personal data breach.

Consideration must also be given to who to notify, what to tell them and how to communicate

the message. This will depend to a large extent on the nature of the personal data breach.

The following factors will be relevant to making a decision:

- Is the personal data breach likely to require notification to a regulatory body for example, Care Inspectorate, Scottish Housing Regulator and / or the Information Commissioner's Office;
- Consider the most appropriate way to notify those individuals affected, the security of the chosen medium for communication as well as the urgency of the situation
- The notification should at the very least detail how and when the personal data breach occurred and the data involved. This should include details of what has already been done to respond to the risks posed by the personal data breach;
- When notifying individuals, specific and clear advice must be given on what steps can be taken by the individuals concerned to protect themselves and also what can be done to help them;
- How we might provide a way for individuals to receive further information or to ask questions about the personal data breach incident. For example, a helpline number, web page or contact; and
- Consideration should also be given to notifying third parties such as the police, insurers, professional bodies, unions and bank or credit card companies who can assist in reducing the risk of loss.

Whether notification of the Information Commissioner's Office is required will be dependent on the facts and circumstances of the personal data breach **and shall be determined by the Data Protection Officer**. Examples of where the Information Governance Team will require to notify the Information Commissioner's Office include where there are a large number of people affected or there are potentially serious consequences following on from the personal data breach, i.e. there is a risk to the rights and freedoms of individuals as a result of the personal data breach. Notifications to the Information Commissioner's Office under the Data Protection Legislation must contain details of the nature of the personal data breach, including the categories and number of individuals and numbers of personal data records concerned; contact details for the Group; the likely consequences of the personal data breach; and the measures taken, or proposed to be taken, to deal with the personal data breach and mitigate against any adverse effects.

## Evaluation and Response

It is important not only to investigate the causes of any personal data breach but to also evaluate the effectiveness of the response to it. The purpose of the review is to ensure that the steps taken during the incident were appropriate and to identify areas that may need to be improved.

**In completing the evaluation, the following should be considered:**

- Did the relevant business area know what personal data was held, where it was held, how long it had been held and how it was stored?
- Where are the greatest risks? For example, is special categories of personal data or financial information held? If so, how secure are the storage arrangements and is it stored across the business or in a single location?
- Can weaknesses in existing security measures for paper and electronic information be identified?

- Risks arise when sharing personal information with or disclosing to other parties. Is the method of transmission secure, is the minimum amount of personal information shared to fulfil the purposes and is there a record or audit trail of the disclosure? Is a data sharing agreement in place? Has it been adhered to and / or does it require review or additional monitoring?
- Any recommended changes to policies or procedures should be documented and implemented as soon as possible following the personal data breach;
- Was there a group or individual, within the business division, identified to respond to an actual or suspected personal data breach and was the group adequately skilled to do so? For example, did the group / individual have the necessary awareness of security issues or is there a need for training or tailored advice? and
- In the case of a serious incident, was there a need to refer to the Business Continuity Plan and is there a need to develop a similar plan for possible future personal data breaches?

The evaluation should be carried out within a reasonable timescale and reported back to the Director of Finance and Corporate Services, together with any recommendations identified for improvement and a timeline for implementation of such recommendations.

**Appendix 4**

**Guidance on Individuals' Rights**

**Right to be informed**

The **right to be informed** requires transparency of the Group's personal information and is achieved through providing certain information contained in privacy notices and statements to individuals. The Group has published privacy notices for the different categories of information collected. These privacy notices comply with the requirements of the Data Protection Legislation

The following information must be given to individuals when their personal information is requested:

- Identity of and contact details for the Group entity that is the Controller of their personal information (including the Data Protection Officer);
- Details on the reasons for and how their personal information will be used, with reference to one of the legal grounds for Processing in the GDPR (including the legitimate interests of the Group, if applicable);
- Any recipient or categories of recipient of their personal information;
- Details on any transfer of their personal information outside the EU and the safeguards the Group has in place for such transfer;
- The retention period for their personal information or the criteria used to determine how long their personal information is held by the Group;
- Details of each right the individual has, including the right to withdraw any consent they have given and complain to the Information Commissioner's Office; and
- If their personal information is required by a statutory or contractual requirement and possible consequences of failing to provide their personal information.

Individuals must be provided with a copy of the privacy notice, a link to a privacy notice or separate privacy statement when their personal information is being collected by the Group. For example, a request for housing application form should include a Privacy Notice with the above information.

If the Group obtains an individual's personal information from anyone other than the individual who is the subject of the personal information, the Group must make accessible a privacy notice to that individual within a reasonable period after obtaining their personal information, but at the latest within one month. Such a notice will need to include the details listed above, as well as information on the categories of personal information processed by the Group and the source of their personal information.

The Data Protection Officer has template wording and is responsible for reviewing any information before it is provided to individuals. If you are unsure whether an individual needs to be given a privacy notice, please contact the Data Protection Officer before asking the individual for any personal information.

**Right of access**

The **right of access** allows an individual to obtain information regarding and a copy of their personal information processed by the Group. This includes electronic and paper records as well as CCTV and audio recordings. The Group has procedures in place to ensure that individuals (and their authorised representatives), who make an application for information held about them, known as a 'subject access request', will be provided with all relevant information, to which they are entitled by law (subject to statutory exemptions).

All individuals making a subject access request should be asked to do so in writing or by using our subject access request form. The subject access request form can be found on our website together with guidance on subject access requests.

The Data Protection Officer is responsible for the administration of all subject access requests for the Group. Any subject access requests received must be provided to the Data Protection Officer **immediately** upon receipt. The Data Protection Officer shall respond to each subject access request within the statutory time limit for doing so, which is within one month.

## Right to rectification

The **right to rectification** gives individuals a right to have their personal information corrected if it is inaccurate or incomplete. When the Group receives a request from an individual to rectify their personal information, we have one month to respond (this can be extended by two months for complex requests).

If the Group complies with this request, any third parties who have received the relevant personal information must be informed of the rectification if possible and details of any such third parties must be given to the individual.

If the Group decides not to take action in response to a request for rectification, we must explain why to the individual and let them know that they can complain to the Information Commissioner's Office or seek a remedy through the courts.

Any requests for rectification must be provided to the Data Protection Officer **immediately** upon receipt, together with a copy of the relevant personal information and any comments relating to its accuracy.

Most requests to update personal information – for example, where a tenant / service user provides the Group with updated contact details – will be able to be dealt with on a day-to-day basis. However, any official requests that reference the Data Protection Legislation, contain extensive amendments, or relate to personal information that the Group feels is accurate should be passed to the Data Protection Officer to respond.

## Right to erasure

The **right to erasure** is also known as the 'right to be forgotten' and allows an individual to request that the Group deletes or removes their personal information where there is no compelling reason to continuing processing it.

This right applies in the following circumstances:

- Where the personal information is no longer necessary for the purposes it was originally collected / processed;
- When the basis for processing the individual's personal information is consent that they withdraw their consent;
- When the individual objects to the processing of their personal information and the Group does not have an overriding legitimate interest to continue the processing;
- The personal information was unlawfully processed – i.e. in breach of the Data Protection Legislation;
- The personal information has to be deleted in order to comply with a legal obligation;

and

- The personal information is processed in relation to targeting online services to a child.

The Data Protection Officer has responsibility for determining whether a request for erasure can be complied with. The Group has one month to respond to requests from data subject exercising this right, but this can be extended by a further two months if the request is complex or the Group has received a number of requests from the data subject. There are certain circumstances when the Group can refuse a request for erasure, such as when the personal information is processed for the following reasons:

- To exercise the right of freedom of expression and information;
- To comply with a legal obligation to perform a public interest task or exercise official authority;
- For public health purposes in the public interest;
- For archiving purposes in the public interest, scientific research, historical research or statistical purposes; or
- To exercise or defend legal claims.

If the Group deletes any personal information following a request for erasure that has been disclosed to third parties, the Group must inform the third parties about the deletion, unless it is impossible or involves disproportionate effort to do so.

Any requests for erasure must be provided to the Data Protection Officer upon receipt, together with a copy of the relevant personal information and any comments relating to the reasons for processing it.

**Right to restrict Processing**

The **right to restrict processing** allows individuals to request that the Group restricts the Processing of their personal information. The Group has one month to respond to requests from data subject exercising this right, but this can be extended by a further two months if the request is complex or the Group has received a number of requests from the data subject. When processing is restricted, the Group can still store the individual's personal information but cannot process it anymore.

The Group will need to restrict the processing of personal information in the following circumstances:

- When an individual claim that the personal information is inaccurate, the processing of that personal information should be restricted until the accuracy of it is verified;
- When the Group is considering if our legitimate interests override those of the individual where the individual has objected to the processing of their personal information;
- When the Group's processing is unlawful and the individual requests restriction of the processing of their personal information rather than erasure; and
- When the Group no longer needs the personal information but the individual requires their personal information to establish, exercise or defend a legal claim.

The Data Protection Officer is responsible for determining if any processing of personal

information is to be restricted and any requests for restriction must be provided to the Data Protection Officer upon receipt, together with a copy of the relevant personal information and any information regarding the processing.

**Right to data portability**

The **right to data portability** allows individuals to obtain their personal information from the Group and reuse it for their own purposes. The Group has one month to respond to requests from data subject exercising this right, but this can be extended by a further two months if the request is complex or the Group has received a number of requests from the data subject. For example, this could apply to a tenant moving between landlords or an employee moving between employers.

This right only applies to personal information provided to the Group by an individual, where the Group processes the personal information based on the individual's consent or in order to perform a contract, and the processing is carried out by automated means (i.e. inputted into any of the Group's IT systems).

The Group has one month to respond to requests for data portability and the Data Protection Officer has responsibility for responding to these. Any requests for data portability must be passed to the Data Protection Officer **immediately**, together with a copy of the personal information requested by the individual.

**Right to object**

Individuals have the **right to object** to the Group's processing of their personal information. The Group has one month to respond to requests from data subject exercising this right, but this can be extended by a further two months if the request is complex or the Group has received a number of requests from the data subject. The right to object can be exercised where personal information is used for:

- Legitimate interests or to perform a task in the public interest / exercise of official authority:
    - Individuals can object for reasons relating to their particular situation; and
    - The Group must stop processing the personal information unless our legitimate interests override those of the individual or the processing is to establish, exercise or defend legal claims;
- Direct marketing:
    - As soon as the Group receives an object to direct marketing activities, we must stop processing the individual's personal information for direct marketing purposes **immediately**; and

- Scientific / Historic research and statistics:
    - Individuals can object for reasons relating to their particular situation; and
    - The Group is not required to comply with an objection where the processing of personal information in necessary for the performance of a public interest task.

The Data Protection Officer has responsibility for dealing with objections to processing and any objections to processing personal information must be passed to the Data Protection Officer **immediately**, together with a copy of the personal information details of the processing objected