DATA PROTECTION POLICY

Document information		
Version Number	V2	
Type	Operating Procedure ☐ Corporate Policy ☒	Customer Policy ☐ Staffing Policy ☐
Scope	Albyn Group ☒ Albyn Housing Society ☐	Highland Residential ☐
Approver	Board ☒	Leadership Team ☐
Responsible Director	Audrey Murphy	
File Location	Policy & Procedures SharePoint folder	
Approval & Publication		
Approval Date	21/03/2023	
Date of next planned review	31/03/2028	
For website publication (Y/N)	Yes	
Distribution	All Staff ☒ Customers ☒ Albyn Board ☒ Highland Residential Board ☒	Finance & Corporate Services ☐ Human Resources ☐ Property Services & Subsidiaries ☐ Customer Services ☐ Highland Residential ☐

Summary of changes to document				
Date	**Action by**	**Version updated**	**New version number**	**Brief description** ***(e.g., updated job titles, reviewed section on delivery, whole document updated, corrected typos)***
02/2023	Corporate Officer	V1	V2	Adoption of SFHA model policy

CONTENTS

1.0 Introduction

Albyn Group (the "Group") is committed to ensuring the secure and safe management of data held in relation to customers, staff, and other individuals. The Group's staff members have a responsibility to ensure compliance with the terms of this policy, and to manage individuals' data in accordance with the procedures outlined in this policy and documentation referred to herein.

The Group needs to gather and use certain information about individuals. These can include customers (tenants, factored owners etc.), employees, and other individuals that the Group has a relationship with. The Group manages a significant amount of data, from a variety of sources. This data contains Personal Data and Sensitive Personal Data (known as Special Categories of Personal Data under the UK GDPR).

This policy sets out the Group's duties in processing that data, and the purpose of this policy is to set out the procedures for the management of such data.

2.0 Legislation

It is a legal requirement that the Group must collect, handle and store personal information in accordance with relevant legislation.

The relevant legislation in relation to the processing of data is:

(a) the UK General Data Protection Regulation ("the GDPR")
(b) the Privacy and Electronic Communications (EC Directive) Regulations 2003 (as may be amended by the proposed Regulation on Privacy and Electronic Communications)
(c) the Data Protection Act 2018 ("the DPA")
(d) any legislation that, in respect of the United Kingdom, replaces, or enacts into United Kingdom domestic law, the UK General Data Protection Regulation, the proposed Regulation on Privacy and Electronic Communications or any other law relating to data protection, the processing of personal data and privacy as a consequence of the United Kingdom leaving the European Union.

3.0 Data

The Group holds a variety of Data relating to individuals, including customers and employees (also referred to as Data Subjects). Data which can identify Data Subjects is known as Personal Data. The Personal Data held and processed by the Group is detailed within its Privacy Notices, as well as within Terms of and Conditions of Employment.

"Personal Data" is that from which a living individual can be identified either by that data alone, or in conjunction with other data held by the Group.

The Group also holds Personal Data that is sensitive in nature (i.e., relates to or reveals a data subject's racial or ethnic origin, religious beliefs, political opinions, relates to health or sexual orientation). This is "Special Category Personal Data" or "Sensitive Personal Data".

4.0 Processing of Personal Data

The Group is permitted to process Personal Data on behalf of Data Subjects provided it is doing so on one of the following grounds:

- Processing with the consent of the Data Subject
- Processing is necessary for the performance of a contract between the Group and the Data Subject or for entering into a contract with them.
- Processing is necessary for the Group's compliance with a legal obligation.

- Processing is necessary to protect the vital interests of the Data Subject or another person; or
- Processing is necessary for the performance of a task carried out in the public interest or in the exercise of the Group's official authority.

4.1 Privacy Notices

The Group is required to provide Privacy Notices to all customers whose Personal Data is held by the Group. The Privacy Notice must be provided to the customer from the outset of the processing of their Personal Data and they should be advised of the terms of the Privacy Notice when it is provided to them. Privacy Notices are available on the Albyn Housing Society and Highland Residential (Inverness) Ltd websites.

4.2 Employees

Employee Personal Data and, where applicable, Special Category Personal Data or Sensitive Personal Data, is held and processed by the Group. Details of the data held and processing of that data is contained within the Employee Privacy Notice which is provided to all employees at point of contract. Prospective employees are provided with a Recruitment Privacy Notice at point of application. A copy of any employee's Personal Data held by the Group is available upon request by that employee from the Group Data Protection Officer.

4.3 Consent

Consent as a ground of processing will require to be used from time to time by the Group when processing Personal Data. It should be used by the Group where no other alternative ground for processing is available. In the event that the Group requires to obtain consent to process a Data Subject's Personal Data, it shall obtain that consent in writing. The consent provided by the Data Subject must be freely given and the Data Subject will be required to sign a relevant consent form if willing to consent. Any consent to be obtained by the Group must be for a specific and defined purpose (i.e., general consent cannot be sought). Where consent is being relied on, Data Subjects are free to withhold their consent or withdraw it at any future time.

4.4 Processing of Special Category Personal Data or Sensitive Personal Data

In the event that the Group processes Special Category Personal Data or Sensitive Personal Data, the Group must rely on an additional ground for processing in accordance with one of the special category grounds.

Schedule 1 Part 4 of the DPA requires the Group to have in place an Appropriate Policy Document when it relies on certain conditions for processing Special Category and Criminal Offence data. Further details are provided within the Group Special Category & Criminal Offences Data Processing Policy provided in Appendix A.

5.0 Data Sharing

The Group shares its data with various third parties for numerous reasons in order that its day-to-day activities are carried out in accordance with the Group's relevant policies and procedures. In order that the Group can monitor compliance by these third parties with Data Protection laws, the Group may require the third party organisations to enter in to an agreement with the Group governing the processing of data, security measures to be implemented, and responsibility for breaches. This will only apply in situations where the third party is a joint controller.

5.1 Data Sharing Agreements

Personal Data is from time-to-time shared amongst the Group and third parties who require to process the same Personal Data as the Group. Whilst the Group and third parties may jointly determine the purposes and means of processing, both the Group and the third party will be processing that data in their individual capacities as data controllers.

Where the Group shares in the processing of personal data with a third party organisation (e.g. for processing of the employees' pension), it shall require the third party organisation to enter in to a Data Sharing Agreement with the Group.

5.2 Data Processing Agreements

A data processor is a third-party entity that processes Personal Data on behalf of the Group and is frequently engaged if certain of the Group's work is outsourced (e.g. payroll, maintenance and repair works).

A data processor must comply with Data Protection laws. The Group's data processors must ensure they have appropriate technical security measures in place, maintain records of processing activities and notify the Group if a data breach is suffered.

If a data processor wishes to sub-contact their processing, prior written consent of the Group must be obtained. Upon a sub-contracting of processing, the data processor will be liable in full for the data protection breaches of their sub-contractors.

Where the Group contracts with a third party to process personal data held by the Group, it shall require the third party to enter in to a Data Protection Addendum with the Group.

6.0 Data Storage and Security

All Personal Data held by the Group must be stored securely, whether electronically or in hard copy format.

6.1 Paper Storage

If Personal Data is stored on paper it should be kept in a secure place where unauthorised personnel cannot access it. Employees should ensure that no Personal Data is left in a place where unauthorised personnel can access it. When the Personal Data is no longer required it must be disposed of by the employee so as to ensure its secure destruction. If the Personal Data requires to be retained on a physical file then the employee should ensure that it is affixed to the file which is then stored in accordance with the Group's storage provisions.

6.2 Electronic Storage

Personal Data stored electronically must also be protected from unauthorised use and access. Personal Data should be password protected when being sent internally or externally to the Group's data processors or those with whom the Group has entered in to a Data Sharing Agreement. If Personal Data is stored on removable media (CD, DVD, USB memory stick) then that removable media must be encrypted and stored securely at all times when not being used. Personal Data should not be saved directly to mobile devices and should be stored on designated drivers and servers.

7.0 Breaches

A data breach can occur at any point when handling Personal Data and the Group 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.

7.1 Internal Reporting of Breaches

The Group 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 hours after it has occurred, the Group's 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 Group must seek to contain the breach by whichever means available.
- The DPO 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.
- Notify third parties in accordance with the terms of any applicable Data Sharing Agreements.

7.2 Reporting Breaches 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.

8.0 Data Protection Officer ("DPO")

A Data Protection Officer is an individual who has an over-arching responsibility and oversight over compliance by the Group with Data Protection laws. The Group has appointed a Data Protection Officer (DPO). The Group's DPO's details are noted on the Group's website and contained within all Privacy Notices.

The DPO will be responsible for:

- Monitoring the Group's compliance with Data Protection laws and this Policy.
- Co-operating with and serving as the Group's contact for discussions with the ICO.
- Reporting breaches or suspected breaches to the ICO and Data Subjects.

9.0 Data Subject Rights

Certain rights are provided to Data Subjects under the GDPR. Data Subjects are entitled to view the Personal Data held about them by the Group, whether in written or electronic form.

Data Subjects have a right to request a restriction of processing their data, a right to request erasure of their Personal Data, and a right to object to the Group's processing of their data. These rights are notified to the Group's tenants and other customers in the Group's Privacy Notices. Such rights are subject to qualification and are not absolute.

9.1 Subject Access Requests

Data Subjects are permitted to view their Personal Data held by the Group upon making a request to do so (a Subject Access Request). Upon receipt of a request by a Data Subject, the Group must respond to the Subject Access Request within one month from the day after the date of receipt of the request. The Group:

- Must provide the Data Subject with an electronic or hard copy of the Personal Data requested, unless any exemption to the provision of that data applies in law.

- Where the Personal Data comprises data relating to other Data Subjects, must take reasonable steps to obtain consent from those Data Subjects to the disclosure of that Personal Data to the Data Subject who has made the Subject Access Request.
- Where the Group does not hold the Personal Data sought by the Data Subject, must confirm that it does not hold any or that Personal Data sought to the Data Subject as soon as practicably possible, and in any event, not later than one month from the day after the date on which the request was made.

9.2 The Right to Erasure

A Data Subject can exercise their right to erasure (otherwise known as the right to be forgotten) by submitting a request to the Group seeking that the Group erase the Data Subject's Personal Data in its entirety.

Each request received by the Group will require to be considered on its own merits and legal advice will require to be obtained in relation to such requests from time to time. The DPO will have responsibility for accepting or refusing the Data Subject's request and will respond in writing to the request.

Requests for erasure will be considered and responded to by the Group by one month from the day after the date we receive the request.

9.3 The Right to Restrict or Object to Processing

A Data Subject may request that the Group restrict its processing of the Data Subject's Personal Data, or object to the processing of that data.

In the event that any direct marketing is undertaken from time-to-time by the Group, a Data Subject has an absolute right to object to processing of this nature by the Group, and if the Group receives a written request to cease processing for this purpose, then it must do so immediately.

Each request received by the Group will require to be considered on its own merits and legal advice will require to be obtained in relation to such requests from time to time. The DPO will have responsibility for accepting or refusing the Data Subject's request and will respond in writing to the request.

9.4 The Right to Rectification

A Data Subject may request the Group to have inaccurate Personal Data rectified. If appropriate, a Data Subject may also request the Group to have incomplete Personal Data completed.

Each request received by the Group will require to be considered on its own merits and legal advice will require to be obtained in relation to such requests from time to time. The DPO will have responsibility for accepting or refusing the Data Subject's request and will respond in writing to the request.

10.0 Data Protection Impact Assessments ("DPIAs")

These are a means of assisting the Group in identifying and reducing the risks that our operations have on personal privacy of Data Subjects. The Group shall:

- Carry out a DPIA before undertaking a project or processing activity which poses a "high risk" to an individual's privacy. High risk can include, but is not limited to, activities using information relating to health or race, or the implementation of a new IT system for storing and accessing Personal Data.

- In carrying out a DPIA, include a description of the processing activity, its purpose, an assessment of the need for the processing, a summary of the risks identified and the measures that it will take to reduce those risks, and details of any security measures that require to be taken to protect the Personal Data
- The Group will require to consult the ICO in the event that a DPIA identifies a high level of risk which cannot be reduced or mitigated. The DPO will be responsible for such reporting, and where a high level of risk is identified by those carrying out the DPIA they require to notify the DPO within five (5) working days.

11.0 Archiving, Retention and Destruction of Data

The Group cannot store and retain Personal Data indefinitely. It must ensure that Personal Data is only retained for the period necessary. The Group shall ensure that all Personal Data is archived and destroyed in accordance with the periods specified within the Group Data Retention Schedule.

12.0 Review

This policy will be reviewed in 5 years, or earlier if required.

APPENDIX A: SPECIAL CATEGORY & CRIMINAL OFFENCES DATA PROCESSING POLICY

1.0 Introduction

As part of Albyn Housing Society's functions as a Registered Social Landlord, it processes Special Category data and Criminal Offence data in accordance with the requirements of Article 9 and 10 of the General Data Protection Regulation ('GDPR') and Schedule 1 of the Data Protection Act 2018 ('DPA').

Schedule 1 Part 4 of the DPA requires Albyn to have in place this document, called an Appropriate Policy Document (APD), when it relies on certain conditions for processing Special Category and Criminal Offence data. This policy will tell you what Special Category and Criminal Offence data Albyn processes, its lawful basis (schedule 1 condition in the DPA) for processing it, the purposes for which it processes it, and how it ensures compliance with the principles of data protection law provided in Article 5 of the GDPR.

This policy is applicable to the trading subsidiaries of Albyn Housing Society, to be referred to hereinafter as 'Albyn'.

2.0 Description of Special Category and Criminal Offence Data Processed

Special category data means information about an individual's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health, sex life or sexual orientation and genetic or biometric data.

Criminal records data means information about an individual's criminal convictions and offences, and information relating to criminal allegations and proceedings.

3.0 Description of Data Processed

Albyn processes the special category data about its employees that is necessary to fulfil its obligations as an employer. This includes information about their health and wellbeing, ethnicity, photographs and their membership of any trade union. Further information about this processing can be found in the Employee Privacy Notice and Recruitment Process Privacy Notice.

Albyn processing for reasons of substantial public interest relates to the data it receives or obtains in order to fulfil its function as a Registered Social Landlord. Further information about this processing can be found in the Customer Privacy Notice.

4.0 Conditions for Processing

Below are listed the DPA Schedule 1 conditions on which Albyn is relying to process special category and criminal offence data.

- **Schedule 1 Part 1 Paragraph 1 - Employment, social security and social protection.**
  Example of processing includes staff sickness records and requesting criminal records checks as part of the recruitment process.

- **Schedule 1 Part 2 Paragraph 6 - Statutory, etc. purposes**
  Example of processing includes where Albyn needs to process data for the purposes of performing its function as a Registered Social Landlord.

- **Schedule 1 Part 2 Paragraph 8 – Equality of opportunity**
  Example of processing includes the collection of equality information in order to promote equal opportunities.

- **Schedule 1 Part 2 Paragraph 10 - Preventing or detecting unlawful acts.**
  Example of processing includes where Albyn report matters to the Police, local authorities or other regulatory bodies.

- **Schedule 1 Part 2 Paragraph 12 - Regulatory requirements relating to unlawful acts and dishonesty.**
  Example of processing includes where Albyn reports matters to regulatory authorities or assist with their investigations.

- **Schedule 1 Part 2 Paragraph 18 - Safeguarding of children and individuals at risk.**
  Example of processing includes where Albyn receives reports of customers at risk and needs to take steps to ensure their safety.

- **Schedule 1 Part 2 Paragraph 24 - Disclosure to elected representatives**
  Example of processing includes responding to requests for information from MSPs acting on behalf of their local constituent.

5.0 How Albyn complies with the data protection principles in Article 5 of the GDPR

Article 5(2) of the GDPR requires Data Controllers to demonstrate how they comply with the data protection principles provided in Article 5(1). This section illustrates the measures Albyn has taken to demonstrate accountability for the personal data it processes and contains details about how it ensures compliance with the principles of the GDPR.

5.1 Accountability

Albyn has put in place appropriate technical and organisational measures to meet the requirements of accountability. These include:

- The appointment of a Data Protection Officer who reports directly to our highest management level.
- Taking a 'data protection by design and default' approach to its activities.
- Maintaining documentation of its processing activities.
- Adopting and implementing data protection policies and ensuring it has written contracts in place with our data processors.
- Implementing appropriate security measures in relation to the personal data it processes.
- Carrying out data protection impact assessments for high-risk processing.

5.2 Lawful, fair and transparent processing

Albyn provides clear and transparent information to individuals about why it processes their personal data, including the lawful basis in its Privacy Notices. This includes information about why Albyn processes Special Category and Criminal Offence data.

As a Registered Social Landlord Albyn needs to process special category and criminal offence data to meet the requirements of legislation such as the Housing (Scotland) Act (2010), the Equality Act (2010), the Health and Safety Act (1974), and legislation relating to safeguarding.

Albyn processes employment data to meet our legal obligations as an employer.

5.3 Purpose limitation

We process special category and criminal offences data for purposes explained in section 4.

Albyn will not process any personal data for purposes which would be incompatible with the purpose for which the data was originally collected.

5.4 Data minimisation

Albyn collects personal data necessary for the relevant purposes and ensures it is not excessive. The information Albyn processes is necessary for and proportionate to our purposes.

5.5 Accuracy

When Albyn identify data which is inaccurate or out of date, having due regard for the purpose for which the data was processed, it will take necessary steps to rectify, replace or erase it as soon as possible and within one month. If there is a specific reason Albyn cannot rectify or erase the data, for instance because the lawful basis does not permit it, it will record the decision.

5.6 Storage limitation

Special Category and Criminal Offence data processed by Albyn for the purpose of employment or substantial public interest, will be retained for the periods set out in the Albyn Group Retention Policy.

5.7 Security

Electronic information is processed within our secure network. Hard copy information is processed in line with our security procedures.

Our electronic systems and physical storage have appropriate access controls applied.