

**Information Security Policy**

|  |  |
| --- | --- |
| **Policy Name** | Information Security Policy |
| **Policy Ref** |  |
| **Review Date** | July 2024 |
| **Purpose** | REVIEW & APPROVE |
| **Next Review Date** | July 2027 |
| **Committee** | Board of Management  |
| **Author** | Daradjeet Jagpal (DPO) & Alison Geoghans |
| **Internal Policy** |  | **To be published** | X |

Angus Housing Association Registered Charity Number SC020981

|  |  |
| --- | --- |
| **Scottish Social Housing Charter** **Outcomes** | Number(s) |
|  **The Customer/landlord relationship** | 1.Equalities 2.Communication3.Participation4.Quality of Housing5.Repairs, Maintenance and Improvements6. Estate Management, Anti-Social Behaviour, Neighbour Nuisance and Tenancy Disputes7,8 & 9 Housing Options11. Tenancy Sustainment |

|  |  |
| --- | --- |
| **Written By** | Daradjeet Jagpal |
| **Department** | Corporate |

|  |  |
| --- | --- |
| **Approval Date by Committee** | 21st August 2024 |

|  |  |
| --- | --- |
| **Notes** |  |
| We will comply with all relevant legislation and associated regulations, including:Current Data Protection LegislationReference made to the following sources and other guidance:Data Protection PolicyData Retention PolicyData Subject Requests* Failure by Angus HA to comply with data protection law could result in Angus HA being exposed to enforcement action by the Information Commissioner’s Office and possibly a monetary penalty.
* Breach of data protection law could reduce public trust and confidence in the work of Angus HA and lead to loss of reputation and negative publicity.
* Use of rights contained within data protection law could impose a significant resource burden on Angus HA.
* A serious breach of data protection law is a notifiable event to the Scottish Housing Regulator.

  |

**ANGUS HOUSING ASSOCIATION LIMITED**

**INFORMATION SECURITY POLICY**

Introduction

* 1. We are committed to the highest standards of information security.
	2. Data protection legislation requires us to:
		1. use technical and organisational measures to ensure personal data is kept secure, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage to personal data;
		2. implement appropriate technical and organisational measures to demonstrate that we have considered and integrated data protection compliance measures into our personal data processing activities; and
		3. demonstrate that we have used or implemented such measures.
	3. The purpose of this Policy is to:
		1. protect against potential breaches of confidentiality;
		2. ensure all our information assets and IT facilities are protected against damage, loss or misuse;
		3. supplement our Data Protection Policy to ensure that all staff are aware of and comply with data protection legislation as part of their roles at our organisation; and
		4. increase awareness and understanding within the organisation of the requirements of information security and the responsibility of staff to protect the confidentiality and integrity of the personal data that they handle and use as part of their roles.
	4. This Policy supplements our Data Protection Policy and other relevant procedures (including the Data Breach Management Procedure) and transparency statements, and the contents of those policies and statements must be considered, as well as this Policy.

Definitions

For the purposes of this Policy:

|  |  |
| --- | --- |
| business information  | 1. means business-related information, other than personal data relating to housing applicants, our tenants (and their household members), sharing owners, factored owners, job applicants, current and former employees, contractors, business contacts (including at other registered social landlords, regulators, local authorities and agencies), complainants, elected members, apprentices, committee members, and members;
 |
| confidential information  | 1. means trade secrets or other confidential information (either belonging to us or to third parties); and
 |
| personal data  | 1. means information relating to an individual who can be identified (directly or indirectly) from that information.
 |

Roles and responsibilities

* 1. Information security is the responsibility of all our staff. Our Data Protection Officer (DPO) is responsible for:
		1. monitoring and implementing this Policy;
		2. monitoring potential and actual security breaches;
		3. ensuring that staff are aware of their responsibilities through training and issuing guidance and communications to them; and
		4. ensuring compliance with data protection legislation and guidance issued by the Information Commissioner’s Office.

Scope

* 1. The information covered by this Policy includes all written, spoken and electronic information held, used or transmitted by or on our behalf, in whatever media. This includes information held on computer systems, hand-held devices, phones, paper records, and information transmitted orally.
	2. This Policy applies to all staff.
	3. All staff must be familiar with this Policy and comply with its terms when undertaking their roles with the organisation.
	4. Information covered by this Policy may include:
		1. personal data relating to housing applicants, our tenants (and their household members), sharing owners, factored owners, job applicants, current and former employees, contractors, business contacts (including at other registered social landlords, regulators, local authorities and agencies), complainants, elected members, apprentices, committee members, and members;
		2. other business information; and
		3. confidential information.

General principles

* 1. All our information must be treated as commercially valuable and protected from loss, theft, misuse or inappropriate access or disclosure.
	2. Personal data must be protected against unauthorised and / or unlawful processing and against accidental loss, destruction or damage, using appropriate technical and organisational measures.
	3. Staff should discuss with the DPO the appropriate security arrangements and technical and organisational measures which are appropriate and in place for the type of information that they access as part of their roles at the organisation.
	4. Our information is owned by the organisation and not by any individual or department within the organisation. Our information must be used only in connection with work being carried out for the organisation and not for other commercial or personal purpose.
	5. Personal data must be used only for the specified, explicit and legitimate purposes for which it was collected in accordance with data protection legislation.

Information management

* 1. Personal data must be processed in accordance with:
		1. the data protection principles, set out in our Data Protection Policy; and
		2. all other relevant policies.
	2. We will take appropriate technical and organisational measures to ensure that personal data is kept secure and protected against unauthorised or unlawful processing, and against accidental loss, destruction or damage.
	3. Personal data and confidential information will be kept for no longer than is necessary and stored and destroyed in accordance with our Data Retention Procedure.

Human Resources information

* 1. Given the internal confidentiality of personnel files, access to such information is limited to Corporate Services Officer. Other staff are not authorised to access that information.
	2. Any staff member in a management or supervisory role or involved in recruitment must keep personnel information to which they have access strictly confidential during the recruitment process, and must pass this to Corporate Services Officer once the recruitment process is complete.
	3. Staff may ask to see their personnel files and any other personal data in accordance with their rights under data protection legislation. Further information is contained in our Response Procedures for Data Subject Requests and from our DPO.

Access to offices and information

* 1. Office doors and keys and access codes must always be kept secure and keys and access codes must not be given to any third party at any time.
	2. Documents containing confidential information and equipment displaying confidential information should be positioned in a way to avoid them being viewed by people passing by e.g. through ground floor windows. If this cannot be avoided, then blinds should always be positioned to prevent this.
	3. Visitors must be required to sign in at reception, always accompanied and never left alone in areas where they could have access to confidential information.
	4. Wherever possible, visitors should be seen in meeting rooms. If it is necessary for a member of staff to meet with visitors in an office or other room which contains our information, then steps should be taken to ensure that no confidential information is visible.
	5. Whenever possible, at the end of each day, or when desks are unoccupied, documents and devices containing confidential information must be securely locked away.

Computers and IT

* 1. Password protection and encryption must be used, where available, on our systems to maintain confidentiality.
	2. Computers and other electronic devices must be password protected and those passwords must be changed on a regular basis. Passwords must not be written down in places where they are visible or shared with others.
	3. Computers and other electronic devices must be locked when not in use and when staff leave their desks, to minimise the risk of accidental loss or disclosure.
	4. Confidential information must not be copied onto portable media without the express authorisation of Shackleton Technologies Information held on any of these devices should be transferred to our document management system as soon as possible for it to be backed up and then deleted from the device.
	5. Staff must ensure they do not introduce viruses or malicious code on to our systems. Software must not be installed or downloaded from the internet without it first being virus checked and explicitly approved by Shackleton Technologies. Staff should contact Shackleton Technologies for authorisation and guidance on appropriate steps to be taken to ensure compliance.

Disposal of computers and IT equipment

* 1. IT equipment (which includes its storage media) will be disposed of at the end of its useful life. Such equipment may store business information, confidential information and personal data and must therefore be disposed of in a secure manner to protect such information and to ensure that it cannot be accessed post disposal.
	2. Prior to disposal, consideration should be given to whether it is possible to re-use IT equipment within the organisation, wherever possible.
	3. If re-use is not possible, then the IT equipment must be disposed of via our contractor, who will remove the IT equipment from our office and issue a certificate to us to confirm that it has been disposed of securely and that all storage media have been wiped and destroyed. Secure disposal means that the IT equipment is destroyed in a manner that maintains the security of the IT equipment up to the point of destruction. We will only use contractors who provide sufficient guarantees in these regards.
	4. Staff must not attempt to wipe storage media themselves, as deleting a file does not permanently delete it and put it beyond use.
	5. If staff have access to the organisation’s IT equipment at home or use portable devices as part of their roles, then such IT equipment must be returned to the organisation for disposal and must not be retained by staff or otherwise disposed of in domestic recycling or dump facilities.
	6. The organisation will maintain an IT equipment destruction register, recording details of the IT equipment that has been disposed of by the organisation (including the IT equipment’s asset number) and the method of destruction), together with copies of the certificates issued by our contractor under paragraph 10.3.

Communications and transfer of information

* 1. Staff must be careful about maintaining confidentiality when speaking in public places e.g. when speaking in the front office area or outwith the office either in person or via telephone.
	2. Confidential information must be marked “confidential” and circulated only to those who need to know the information during their work for the organisation.
	3. Confidential information must not be removed from our offices, unless required for authorised business purposes, and then only in accordance with paragraph 11.4 below.
	4. Where confidential information is permitted to be removed from our offices, all reasonable steps must be taken to ensure that the integrity and confidentiality of the information are maintained. Staff must ensure that confidential information is:
		1. stored on an encrypted device, which has been authorised by Shackelton Technologies, with strong password protection, and which is kept locked when not in use;
		2. when in paper format, not transported in clear or other unsecured bags or cases;
		3. not read in public places (e.g. waiting rooms, cafes and on public transport); and
		4. not left unattended or in any place where it is at risk (e.g. in conference rooms, car boots and cafes).
	5. Postal and e-mail addresses and telephone numbers should be checked and verified before information is sent to them. Care should be taken with e-mail addresses to ensure that Microsoft Outlook auto-complete features have not inserted incorrect addresses.
	6. All sensitive or particularly confidential information should be encrypted or password protected before being sent by e-mail or be sent by recorded delivery and its delivery tracked.

Personal e-mail and cloud storage accounts

* 1. Personal e-mail accounts, such as Yahoo, Google or Hotmail and cloud storage services, such as Dropbox, iCloud and OneDrive, are vulnerable to hacking. They do not provide the same level of security as the services provided by our own IT systems.
	2. Staff must not use a personal e-mail account or cloud storage account for our business purposes.
	3. If staff need to transfer a large amount of personal data, they should contact the IT service provider for assistance.

Home working

* 1. Staff must not take our information home unless required for authorised business purposes, and then only in accordance with paragraph 13.2 below.
	2. Where staff are permitted to take our information home, staff must ensure that appropriate technical and practical measures are in place within the home to maintain the continued security and confidentiality of that information. In particular:
		1. personal and confidential information must be kept in a secure and locked environment where it cannot be accessed by household members or visitors; and
		2. all personal and confidential information must be returned to and disposed of at the office and not in domestic waste or at public recycling facilities.
	3. Staff must not store confidential information on their home computers and devices.

Transfer to third parties

* 1. Third parties should be used to process our information only in circumstances where appropriate written agreements are in place ensuring that those service providers offer appropriate confidentiality, information security and data protection undertakings. Consideration must be given to whether the third parties will be “processors” for the purposes of data protection legislation. Examples of processers include our contractors, consultants and professional advisers.
	2. Staff involved in setting up new arrangements with third parties or altering existing arrangements should consult the DPO for more information.

Training

* 1. All staff will receive training on information security and confidentiality. New staff will receive training as part of the induction process. Further training will be provided on a regular basis or whenever there is a substantial change in the law or our policy and procedure.
	2. Training is provided by the DPO and attendance is compulsory for all staff at all levels.

Reporting breaches

* 1. All members of staff have an obligation to report actual or potential data protection compliance failures to the DPO. This allows us to:
		1. investigate the failure and take remedial steps, if necessary;
		2. maintain a register of compliance failures; and
		3. make any applicable notifications to the Information Commissioner’s Office, the Scottish Housing Regulator and affected data subjects, if necessary.
	2. Reference should be made to our Data Breach Management Procedure for our reporting procedure.

Consequences of failure to comply with this Policy

* 1. We take compliance with this Policy very seriously. Failure to comply with it puts us at significant risk.
	2. Due to the importance of this Policy, failure to comply with any requirement of it may lead to disciplinary action for a member of staff under our procedures, and this action may result in dismissal for gross misconduct. If an external organisation breaches this Policy, they may have their contract terminated by us with immediate effect.
	3. Any questions or concerns about this Policy should be directed to the DPO.
1. **Review and updates to this Policy**

We will review and update this Policy in accordance with our data protection obligations and we may amend, update or supplement it from time to time and at least every 3 years or earlier, if required by changes in legislation

Last updated: July 2024