INNISFREE HOUSING ASSOCIATION

March 2024

Data Protection Policy and Procedure

DATA PROTECTION POLICY

CONTENT

DATA PROTECTION POLICY

1. Introduction

1.1 Innisfree Housing Association aims to comply with the legal requirements of the Data Protection Legislation. The Data Protection Legislation governs the use of Personal Data and gives individuals statutory access to Personal Data held by us about them. All Personal Data held by Innisfree falls under the scope of the Data Protection Legislation.

1.2 This Data Protection Policy and Procedure sets out how we handle the Personal Data of our Residents, Personnel, suppliers and other third parties. This policy governs the Processing (including disclosure) of Personal Data and privacy and confidentiality in relation to Innisfree's activities as a registered provider of social housing and as an employer.

1.3 This Policy applies to all Personal Data we Process regardless of the media on which that data is stored or whether it relates to past or present Residents, Personnel, supplier contacts, website users or any other Data Subject.

1.4 All Personnel are expected to comply with this Policy. You must read, understand and comply with this Policy when Processing Personal Data on our behalf and attend training on its requirements. This Policy sets out what we expect from you in order for Innisfree to comply with the Data Protection Legislation and other statutory requirements. Your compliance with this Policy is mandatory. This Policy should be read in conjunction with other internal data protection policies and procedures, which must also be complied with, including:

- Subject Access Policy
- Personal Data Breach Policy
- Data Protection Impact Assessment (DPIA) Policy
- Data Retention Policy
- Data Retention Schedule

You can access these other policies here: Innisfree Intranet. Any breach of this Policy may result in disciplinary action.

1.5 This Policy is an internal document and cannot be shared with third parties, Residents, or regulators without prior authorisation from a member of the Senior Management Team (SMT).

1.6 Innisfree is registered with the ICO and supports the objectives of the Data Protection Legislation. Our registration number is: Z7520726.

2. Guidance on the terms used in this Policy and Procedure

2.1 **Automated Decision Making and Profiling**

The making of a decision about a Data Subject based solely on automated means without any human involvement, which produces legal effects or significantly affects an individual, including 'profiling', which is the automated Processing of Personal Data to evaluate certain things about an individual. This may include, for example, evaluating certain personal aspects relating to an individual, in particular to analyse or predict aspects concerning that individual's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements. A common example is the use of automated decision making in job applications, whereby applicants are automatically accepted or rejected based on their answers to prescribed questions.

2.2 **Consent**

Agreement which must be freely given, specific, informed and be an unambiguous indication of the Data Subject's wishes by which they, by a statement or by a clear positive action, signify agreement to the Processing of Personal Data relating to them.

2.3 **Controller**

The person or organisation that determines when, why and how to Process Personal Data. It is responsible for establishing practices and policies in line with the Data Protection Legislation. We are the Controller of all Personal Data relating to Personnel and Personal Data used in our activities as a social housing provider.

2.4 **Criminal Convictions Data**

Personal Data relating to criminal convictions and offences and includes Personal Data relating to criminal allegations and proceedings.

2.5 **Data Protection Legislation**

The UK General Data Protection Regulation ("UK GDPR"), the Data Protection Act 2018 and any guidance issued by the ICO, as updated from time to time.

2.6 **Data Subject**

A living, identified or identifiable individual about whom we hold Personal Data, such as Personnel, Residents, business contacts etc. Data Subjects may be nationals or residents of any country and may have legal rights regarding their Personal Data.

2.7 **DPIA**
A data protection impact assessment, which is a tool used to identify and reduce risks associated with a data Processing activity.

2.8 **Explicit Consent**
Consent which requires a very clear and specific statement (that is, not just action).

2.9 **ICO**
The Information Commissioner's Office, the UK's independent data authority set up to uphold information rights.

2.10 **Personal Data**
Any information relating to a living individual (Data Subject), who: (i) can be identified or are identifiable, directly, or indirectly, from the information in question; or (ii) can be indirectly identified from that information in combination with other information we possess or can reasonably access. Personal Data includes Special Categories of Personal Data and Pseudonymised Personal Data but excludes anonymous data or data that has had the identity of an individual permanently removed. Personal Data can be factual (for example, a name, email address, location or date of birth) or an opinion about that person's actions or behaviour, or details of intentions in respect of them.

2.11 **Personal Data Breach**
Any act or omission that compromises the security, confidentiality, integrity, or availability of Personal Data or the physical, technical, administrative, or organisational safeguards that we or our third-party service providers put in place to protect it. The loss, or unauthorised access, disclosure, or acquisition, of Personal Data is a Personal Data Breach.

2.12 **Personnel**
All Innisfree employees, workers, contractors, agency workers, consultants, directors, and others.

2.13 Privacy Statements (or Fair Processing Notices)
Separate notices setting out information that we must provide to Data Subjects when we collect information about them. These notices may take the form of general privacy statements applicable to a specific group of individuals (for example, employee privacy notices or the website privacy policy) or they may be stand-alone, one-time privacy statements covering Processing related to a specific purpose.

2.14 **Processing (including Process and Processed)**
Any activity that involves the use of Personal Data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data including organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transmitting or transferring Personal Data to third parties.

2.15 **Processor**
A third party engaged by Innisfree as Controller to provide a service which involves the Processing of Personal Data on behalf of Innisfree.

2.16 **Pseudonymisation (including pseudonymised)**
Replacing information that directly or indirectly identifies an individual with one or more artificial identifiers or pseudonyms so that the person to whom the data relates cannot be identified without the use of additional information which is kept separately and secure.

2.17 **Residents**
All Innisfree residents, potential residents, previous residents, applicants (both successful and unsuccessful) and anyone else associated with or living with residents, such as dependents, family members and others living with residents.

2.18 **Special Categories of Personal Data**
Information revealing racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health conditions, sexual life, sexual orientation, biometric or genetic data. This will include:

- All medical issues, whether physical or mental, including HIV/AIDS status and disabilities
- Drugs/substance abuse
- Child abuse
- Domestic violence

3. SCOPE OF THIS POLICY

3.1 We recognise that the correct and lawful treatment of Personal Data will maintain confidence in Innisfree and will provide for successful business operations. Protecting the confidentiality and integrity of Personal Data is a critical responsibility that we take seriously at all times. Innisfree is exposed to potential fines of up to £17.5 million or 4% of total annual turnover, whichever is higher and depending on the breach, for failure to comply with the provisions of the Data Protection Legislation.

3.2 All departments and line managers are responsible for ensuring all Personnel comply with this Policy and need to implement appropriate practices, processes, controls, and training to ensure that compliance.

3.3 The Office Services Manager is responsible for overseeing this Policy and, as applicable, other internal data protection policies. That post is currently held by Anna Ferdinand, and they can be reached at 020 7692 1248.

3.4 Please contact the Office Services Manager on 020 7692 1248 or dataprotection@innisfree.org.uk with any questions about the operation of this Policy or the Data Protection Legislation or if you have any concerns that this Policy is not being or has not been followed. In particular, you must always contact the Office Services Manager in the following circumstances:

- if you are unsure of the lawful basis which you are relying on to Process Personal Data (including the legitimate interests used by Innisfree)
- if you need to rely on Consent and/or need to capture Explicit Consent
- if you need to draft Privacy Statements or provide privacy information
- if you are unsure about the retention period for the Personal Data being Processed
- if you are unsure about what security or other measures you need to implement to protect Personal Data
- if there has been a Personal Data Breach
- if you think Personal Data may be transferred outside the UK
- if you need any assistance dealing with any rights invoked by a Data Subject
- whenever you are engaging in a significant new or changing Processing activity which is likely to require a DPIA or plan to use Personal Data for purposes other than what it was collected for
- if you plan to undertake any activities involving Automated Decision Making or Profiling
- if you need help with any contracts or other areas in relation to sharing Personal Data with third parties (including our vendors)

4. THE DATA PROTECTION PRINCIPLES

4.1 Innisfree must comply with the rules of good information handling, known as the data protection principles, which are set out in the UK GDPR and require Personal Data to be:

- Processed fairly, lawfully and in a transparent manner (Lawfulness, Fairness and Transparency)
- Not kept in a form which permits identification of Data Subjects for longer than is necessary for the purposes for which the data is Processed (Storage Limitation)
- Collected only for specified, explicit and legitimate purposes and not Processed in any manner incompatible with those purposes (Purpose Limitation)
- Processed in a manner that ensures its security using appropriate technical and organisational measures to protect against unauthorised or unlawful Processing and against accidental loss, destruction, or damage (Security, Integrity, and Confidentiality)

- Adequate, relevant, and limited to what is necessary in relation to the purposes for which it is Processed (Data Minimisation)
- Not transferred to another country without appropriate safeguards being in place (Transfer Limitation)
- Accurate and where necessary kept up to date (Accuracy)
- Made available to Data Subjects, allowing Data Subjects to exercise certain rights in relation to their Personal Data (Data Subject's Rights and Requests)

4.2 We are responsible for and must be able to demonstrate compliance with the data protection principles listed above (Accountability).

5. LAWFULNESS, FAIRNESS, AND TRANSPARENCY

5.1 Personal Data must be Processed lawfully, fairly and in a transparent manner in relation to the Data Subject.

5.2 We can only collect, Process, and share Personal Data fairly and lawfully and for specified purposes. The Data Protection Legislation restricts our actions regarding Personal Data to specified lawful purposes. These restrictions are not intended to prevent Processing but ensure that we Process Personal Data fairly and without adversely affecting the Data Subject.

5.3 Innisfree will only Process Personal Data where one of the following lawful purposes is applicable:

- The Data Subject has given their Consent
- The Processing is necessary for the performance of a contract with the Data Subject or to take specific steps before entering into such a contract
- The Processing is necessary for us to comply with a legal obligation
- The Processing is necessary in order to protect the vital interests of the Data Subject or another person, i.e. in order to protect their life
- The processing is necessary in order to pursue Innisfree's legitimate interests or the legitimate interests of a third party (unless this is overridden by the interests of the Data Subject)

5.4 **Special Category Personal Data**

Where we are Processing Special Category Personal Data, we need to ensure that we have an additional lawful purpose, over and above that set out at paragraph 5.3 above. These additional lawful purposes are set out in the UK GDPR and the ones applicable to Innisfree's Processing activities are:

- The Data Subject has given their Explicit Consent;
- The Processing is necessary for employment purposes or for social protection (which includes providing affordable housing and protecting vulnerable individuals in society);
- The Processing is necessary in order to protect the vital interests of the Data Subject or another person, i.e. in order to protect their life, where they are physically or legally incapable of consenting;
- The Processing relates to information made public by the Data Subject;
- The Processing is necessary in the establishment, exercise, or defense of legal claims; or
- The Processing is necessary for reasons of substantial public interest (such as in relation to the administration of justice or preventing or detecting unlawful acts).

5.5 If you are ever unsure if information constitutes Special Category Personal Data, advice should be sought from your line manager/supervisor or the Office Services Manager before any further Processing of that information takes place.

5.6 Interviews and conversations with Personnel and Residents which involve discussion of Special Category Personal Data, or any sensitive information, should, where possible, always be carried out in private. Where this is not possible and the conversation is taking place by phone and other employees are within earshot, you should avoid identifying the Data Subject during the call and keep the contents of the conversation as anonymous as possible. In-person and telephone conversations with individuals which involve the discussion of sensitive information should not take place in open office areas or anywhere publicly accessible.

5.7 **Consent and Explicit Consent**

Where we are relying on Consent to Process Personal Data, there are specific statutory requirements in the Data Protection Legislation which we must comply with.

5.8 A Data Subject consents to Processing of their Personal Data if they clearly indicate agreement to the Processing, either by a statement or positive action. Consent requires affirmative action so silence, pre-ticked boxes or inactivity are unlikely to be sufficient. If Consent is given in a document which deals with other matters, then the Consent must be kept separate from those other matters.

5.9 Data Subjects must be easily able to withdraw Consent to Processing at any time and withdrawal must be promptly honoured. Consent may need to be refreshed if you intend to Process Personal Data for a different and incompatible purpose which was not disclosed when the Data Subject first consented.

5.10 When Processing Special Category Personal Data or Criminal Convictions Data, we will usually rely on a legal basis for Processing other than Explicit Consent or Consent if possible.

5.11 You will need to evidence Consent captured and keep records of all Consents in accordance with our internal policies so that Innisfree can demonstrate compliance with Consent requirements.

5.12 **Transparency**

Under the Data Protection Legislation, we are required to provide detailed, specific information to Data Subjects depending on whether the information was collected directly from Data Subjects or from elsewhere. We do this mainly through our privacy policy, as well as more context specific privacy information (e.g. signage advising that we use CCTV). The key ways in which we provide privacy information are set out below.

5.13 Whenever you collect Personal Data directly from Data Subjects, including for HR or employment purposes, you must provide the Data Subject with all the information required by the Data Protection Legislation including how and why we will use, Process, disclose, protect, and retain that Personal Data through a Privacy Statement which must be presented before or at the time the Data Subject first provides the Personal Data.

5.14 When Personal Data is collected indirectly (for example, from a third party or publicly available source), you must provide the Data Subject with all the information required by the Data Protection Legislation as soon as possible after collecting or receiving the data. You must also check that the Personal Data was collected by the third party in accordance with the Data Protection Legislation and on a basis which contemplates our proposed Processing of that Personal Data.

5.15. If you are collecting Personal Data from Data Subjects, directly or indirectly, then you must provide Data Subjects with the appropriate Privacy Statement, which can be found here: Innisfree Privacy Statement.

5.16. Where we record phone calls, we will include details of the fact that the call is being recorded through a pre-recorded message before the line connects, and also by including details in our privacy statement.

5.17. Privacy information must be concise, transparent, intelligible, easily accessible, and in clear and plain language so that a Data Subject can easily understand them.

6. PURPOSE LIMITATION

6.1 Personal Data must be collected only for specified, explicit and legitimate purposes. It must not be further Processed in any manner incompatible with those purposes.

6.2 You cannot use Personal Data for new, different or incompatible purposes from that disclosed when it was first obtained unless you have informed the Data Subject of the new purposes and they have Consented where necessary.

6.3 If you have any concerns about this, please do speak to your line manager/supervisor or the Office Services Manager.

7. DATA MINIMISATION

7.1 Personal Data must be adequate, relevant, and limited to what is necessary in relation to the purposes for which it is Processed. Our purposes for Processing Personal Data are set out in our Record of Processing Activities and you have a responsibility for ensuring that this is kept up to date.

7.2. You may only Process Personal Data when performing your job duties requires it. You cannot Process Personal Data for any reason unrelated to your job duties.

7.3. You may only collect Personal Data that you require for your job duties: do not collect excessive data. Ensure any Personal Data collected is adequate and relevant for the intended purposes.

7.4. You must ensure that when Personal Data is no longer needed for specified purposes, it is deleted or anonymised in accordance with our internal data retention guidelines.

8. ACCURACY

8.1 Personal Data must be accurate and, where necessary, kept up to date. It must be corrected or deleted without delay when inaccurate.

8.2 One of the key ways we work to ensure accuracy is by using case-management software, Pyramid as a 'single source of the truth'. You must ensure that the Personal Data we use and hold is accurate, complete, kept up to date and relevant to the purpose for which we collected it. A key way of doing that is by Processing data only on designated systems. You must check the accuracy of any Personal Data at the point of collection and at regular intervals afterwards. You must take all reasonable steps to destroy or amend inaccurate or out-of-date Personal Data. We will also make it easy for residents and staff to update obvious details (e.g. bank details, contact details) using our portals and systems.

8.3 To ensure compliance with this principle, Innisfree regularly asks Personnel and Residents to inform us if there are any changes in personal circumstances that need updating on our systems. Housing staff are expected to regularly check basic information with Residents about them and their household to ensure it is accurate on our systems.

8.4 You are expected to inform us of any changes to your Personal Data as soon as possible so that we can update this information.

9. STORAGE LIMITATION

9.1 Personal Data must not be kept in an identifiable form for longer than is necessary for the purposes for which the data is processed.

9.2 Innisfree will maintain retention policies and procedures to ensure Personal Data is deleted after a reasonable time, in line with the purposes for which it was being held and any statutory retention periods. Innisfree has adopted the National Housing Federation's guidelines and retention periods set out in its "Document retention and disposal for housing associations". The paper sets out recommended retention periods for documents including tenancy agreements and former residents' files. You must comply with the retention periods set out in this document and delete information once the retention period has expired, unless there is a legitimate reason to continue Processing the data. The Office Services Manager will have ultimate responsibility for ensuring that information is deleted

once the retention period has expired. A copy of the guidance and retention periods is available from the Finance Director or can be found here: National Housing Federation - Document retention and disposal for housing associations.

9.3 You must not keep Personal Data in a form which permits the identification of the Data Subject for longer than needed for the legitimate business purpose or purposes for which we originally collected it, including for the purpose of satisfying any legal, accounting or reporting requirements.

9.4 You must take all reasonable steps to destroy or erase from our systems all Personal Data that we no longer require in accordance with Innisfree's applicable records retention schedules and policies. This includes requiring third parties to delete that data where applicable.

9.5 You will ensure Data Subjects are informed of the period for which data is stored and how that period is determined in any applicable Privacy Statement.

9.6 Please note that all written warnings will be removed from Personnel files once they have expired.

10. SECURITY, INTEGRITY, AND CONFIDENTIALITY

10.1 Personal Data must be secured by appropriate technical and organisational measures against unauthorised or unlawful Processing, and against accidental loss, destruction, or damage.

10.2 We will develop, implement, and maintain safeguards appropriate to our size, scope and business, our available resources, the amount of Personal Data that we hold and identified risks (including use of encryption and Pseudonymisation where applicable). We will regularly evaluate and test the effectiveness of those safeguards to ensure security of our Processing of Personal Data.

10.3 You are responsible for protecting the Personal Data we hold. You must implement reasonable and appropriate security measures against unlawful or unauthorised Processing of Personal Data and against the accidental loss of, or damage to, Personal Data. You must exercise particular care in protecting Special Categories of Personal Data and Criminal Convictions Data from loss and unauthorised access, use or disclosure.

10.4 You must follow all procedures and technologies we put in place to maintain the security of all Personal Data from the point of collection to the point of destruction. You may only transfer Personal Data to third-party service providers who agree to comply with the required policies and procedures and who agree to put adequate measures in place, as requested.

10.5 You must maintain data security by protecting the confidentiality, integrity and availability of the Personal Data, as follows:

- Confidentiality: ensuring that only people who have a need to know and are authorised to use the Personal Data can access it;
- Integrity: ensuring that Personal Data is accurate and suitable for the purpose for which it is Processed; and
- Availability: ensuring that authorised users are able to access the Personal Data when they need it for authorised purposes.

10.6 All Personnel hard-copy files will be kept in secure cabinets. All soft-copy files will be given a security password so that employees can only gain access to such records where they have a legitimate business need to do so. Any Special Category Personal Data will be marked as 'private and confidential'.

10.7 You must comply with our Information Security Policy and not attempt to circumvent the administrative, physical, and technical safeguards we implement and maintain in accordance with the Data Protection Legislation and relevant standards to protect Personal Data.

11. TRANSFER LIMITATION

11.1 The Data Protection Legislation restricts data transfers to countries outside the UK to ensure that the level of data protection afforded to individuals by the UK legislation is not undermined. You 'transfer' Personal Data when you transmit, send, view or access that data in or to a country different to that in which the data originated.

11.2. You may only transfer Personal Data outside the UK if one of the following conditions is satisfied:

- the UK has issued regulations confirming that the country to which we transfer the Personal Data ensures an adequate level of protection for the Data Subject's rights and freedoms (an 'adequacy regulation' or 'adequacy decision');
- appropriate safeguards are in place such as an international data transfer agreement (IDTA) or standard contractual clauses (including the international data transfer addendum);
- the Data Subject has provided Explicit Consent to the proposed transfer after being informed of any potential risks; or
- the transfer is necessary for one of the other reasons set out in the UK GDPR including the performance of a contract between us and the Data Subject, to establish, exercise or defend legal claims or to protect the vital interests of the Data Subject where the Data Subject is physically or legally incapable of giving Consent and, in some limited cases, for our legitimate interests.

11.3. If you think that a Processing activity may include the transfer of Personal Data outside the UK, you must consult the Office Services Manager in advance of any such transfer. This includes situations where we are proposing to engage a third-party supplier which stores or Processes Personal Data outside the UK.

12. PERSONAL DATA BREACHES

12.1 Reporting a Personal Data Breach

Under the Data Protection Legislation we must notify high risk Personal Data Breaches to the ICO and, in certain instances, the affected Data Subject(s). We want to encourage a proactive reporting culture, including near-misses. This will help us to identify and address emerging problems.

12.2. We have put in place procedures to deal with any suspected Personal Data Breach and will notify Data Subjects or the ICO where we are legally required to do so. You must report all Personal Data Breaches:

- in the first instance, to the Office Services Manager on 020 7692 1248 or dataprotection@innisfree.org.uk
- in the absence of the Office Services Manager, to the Operations Director);

- in the absence of either of the above, to the Chief Executive.

It will ultimately be a decision for the above individuals as to whether a breach is reportable to the ICO or Data Subjects.

12.3. Where a breach is reportable to the ICO, we only have 72 hours to make this report, after becoming aware of the breach. That awareness begins at the point at which you become aware of the breach, not the point at which you report that breach to any of the responsible individuals above. Our failure to notify the ICO of a breach when required to do so can result in us suffering a heavy fine of up to £8.7 million or 2 per cent of turnover. The fine can be combined with the ICO's other corrective powers, such as warnings and reprimands. Therefore, it is vital that you understand how to recognise a Personal Data Breach and how to report it internally.

12.4. All Personal Data Breaches must be recorded in Innisfree's Data Breach Register, even if that breach is not considered 'high risk' or deemed reportable, and therefore it is vital that you report all actual or suspected breaches to any of the individuals listed above at paragraph 12.2 without delay.

12.5 **Identifying a Personal Data Breach**

Personal data breaches can include:

- Access to Personal Data by an unauthorised third party
- Loss of availability of Personal Data
- Deliberate or accidental action (or inaction) by Innisfree or its Personnel
- Alteration of Personal Data without permission
- Sending Personal Data to an incorrect recipient
- Computing devices, or hardcopy papers, containing Personal Data being lost or stolen

12.6 Even if such occurrences are minor and have minimal consequences, they may still constitute a Personal Data Breach under the Data Protection Legislation, for example:

- sending an email containing minimal Personal Data to the wrong recipient, even where that recipient is trusted and has provided assurances that the email has been deleted;
- losing or misplacing small amounts of paperwork relating to a Resident and their tenancy, even if you are confident that paperwork must be in the office somewhere; or
- accidentally deleting records before the end of Innisfree's internal retention period, such as deleting property maintenance records after two years, where Innisfree's retention period for such information is six years.

12.7. If you know or suspect that a Personal Data Breach has occurred, you must:

- report that breach as soon as possible to any of the individuals listed in paragraph 12.6 above;
- not attempt to investigate the matter yourself;
- preserve all evidence relating to the potential Personal Data Breach; and
- assist the Office Services Manager (or other responsible individual) as far as possible in any investigation, and in the mitigation or remediation of the consequences of the breach.

12.8 **Preventing a Personal Data Breach**

Innisfree works on the premise that prevention is better than cure when it comes to Personal Data Breaches. We have therefore put in place a number of security processes to provide assurances around the integrity of our systems, including through the implementation of robust technical and organisational measures and through the regular auditing of the security of our networks.

12.9 As most Personal Data Breaches are a result of human error or non-compliance with internal policies, we rely on Personnel to take responsibility for their approach to everyday working. There are a number of ways you can help to prevent a Personal Data Breach from occurring in the first place, including:

- Complying with this Policy, our internal [Information Security Policy] and all other policies which relate to the protection of Personal Data and the security of our systems;

13. Monitoring and Review

13.1 The GDPR makes it obligatory for Innisfree to ensure that any personal information it holds on its employees, residents or any other person is accurate and kept up to date (Principle (d) of the GDPR Principles relating to processing of personal data).

13.2 To ensure compliance Innisfree regularly asks its employees and residents to let them know if there have been any changes in personal circumstances so that personal information held on files can be updated.

13.3 No personal information will be kept for longer than is necessary but equally Innisfree will not delete information where there is a genuine business need to retain it.

13.4 All written warnings will be removed from employees' personnel files once they have expired.

13.5 In addition, housing staff will ask residents in interview whether their circumstances have changed and check basic information about them and their household.

13.6 Innisfree has adopted National Housing Federation guidance on the retention of documents contained in the NHF Briefing Paper "Document Retention for Registered Social Landlords". The paper sets out recommended retention periods for documents including tenancy agreements and former residents' files. A copy is available from the Finance Director.

14. Mergers and Acquisitions

14.1 Any information handed over to another organisation in connection with a prospective acquisition or merger will be anonymised. Personal information will be handed over only prior to the final merger or acquisition decision after securing assurances that it will be used solely for the evaluation of assets and liabilities.

14.2 Special categories of personal data will only be disclosed if one of the conditions set out in the GDPR has been satisfied (see Section 3.1 above).

14.3 Employees will be advised wherever practicable if their employment records are to be disclosed to another organisation before an acquisition or merger takes place.

15. Staff Training

15.1 All new staff will receive data protection training as part of their induction into the organisation's workforce and all staff will receive periodic refresher data protection training.

INNISFREE HOUSING ASSOCIATION
190 IVERSON ROAD
LONDON NW6 2HL

Tel: 020 7625 1818

www.innisfree.org.uk

Email: housing@innisfree.org.uk

Version: Data Protection Policy and Procedure March 2024