English Rural

Data Protection and Confidentiality Policy

1. Introduction

1.1 This Policy sets out how English Rural Housing Association will protect the personal information and rights of individuals whose information it uses. It describes the principles and legal obligations to be observed by the Association and partners when collecting and using personal information.

1.2 The lawful and proper treatment of personal information by the Association is important to the success of the business and in order to maintain the confidence of customers, employees and other stakeholders. The principal governing legislation is the General Data Protection Regulation (GDPR) which came into effect in May 2018.

1.3 The principles within this policy apply to any information of a personal nature relating to living individuals that is not a matter of public record and from which a person can be identified. This information may be held on paper or in electronic form, including CCTV footage.

1.4 The duty of confidentiality also extends to any sensitive commercial information relating to the Association or its associates and contractor bodies.

2. Business Strategy

2.1 Compliance with the Data Protection Regulations and other relevant legislation will support the corporate objective of ensuring the business continues to be sustainable and that English Rural has no regulatory intervention.

2.2 Possible risks from breach of this policy will be reflected in the Association's Risk Register.

3. Legislation

3.1 Legislation relevant to this policy includes:

- The Human Rights Act 1998 (the HRA)
- Privacy and Electronic Communications Regulations 2003 (PECR)
- General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679) and the Data Protection Act 2018.

4. Policy Statement

4.1 This policy sets the framework to ensure lawful, proportionate and relevant use of information. Processing which includes collecting; using; protecting and disclosing personal information will be carried out in compliance with the following principles as set out in the GDPR which state that data must be:

- Processed fairly, lawfully and in a transparent way
- Obtained and processed for a specific and legitimate purpose
- Adequate, relevant and limited to what is necessary for the legitimate purposes
- Accurate and kept up to date
- Held for no longer than necessary
- Processed in accordance with the rights of the people whose information is used
- Kept secure from unauthorised processing or disclosure, including by encryption where electronic transmission is used
- Not transferred outside the EU area unless the same safeguards apply.

4.2 In implementing these principles English Rural will:

- Collect and process only the information required to fulfil operational functions or to comply with legal requirements;
- Ensure that only accurate information is collected and kept up to date;
- Ensure that paperwork and computer records are not held for longer than is necessary;
- Take appropriate technical and organisational security measures to safeguard all personal information;
- Ensure that the rights of people about whom the information is held can be fully exercised (see 5.2 below).

4.3 All employees will receive appropriate training to ensure they understand that good data protection practice is their responsibility.

4.4 Access to personal information will be restricted to those employees who need to use it in the course of their work.

4.5 Only in exceptional circumstances will information be shared with third parties without the prior knowledge of the individual concerned (see 5.3 below).

4.6 Those who entrust information to the Association will be told why it is needed, how it will be used and who will have access to it. Where sensitive personal information (see 5.1 below) is required explicit consent to process it will be sought before it is recorded.

4.7 When new technology or methods of recording personal information are to be employed the impact of the change in terms of data protection will be assessed and, if necessary steps will be taken to ensure that data continues to be protected.

4.8 Corporate and commercial information, which is deemed to be sensitive, will be treated as confidential and safeguarded accordingly.

4.9 Secure methods of disposal will be used when personal or sensitive commercial information is no longer required.

4.10 Any breach of this policy will be investigated and this may result in disciplinary action being taken.

4.11 The Association's policy for the retention of personal information is as follows:

o Former HR Files – 10 years

- o Former Tenancy – 5 years
- o Development – 6 years
- o Finance – 7 years
- o Governance – ongoing

4.12 English Rural is committed to being compliant with the General Data Protection Regulation, and will ensure the requirements are considered when reviewing or amending any process which involves personal data.

5. Types and use of personal information

5.1 The principal types of personal information obtained and used by English Rural are as follows:

- Tenants and other members of the tenant's household, the information is *used for the purposes of the contractual relationship between the tenant and English Rural as landlord.*
- Applicants and members of households who are interested in, or seeking housing accommodation or related services from the Association *for the purposes of assessing their housing requirements;*
- Members of staff, workers or contractors, including former staff and prospective members of staff *for the purposes of the employer/employee contractual relationship and compliance with relevant legislation and regulations;*
- Board Members, both current and prospective *for the purposes of recruitment, succession planning and regulatory requirements;*
- People with whom the Association is working *to provide, maintain, promote rural affordable housing;*
- People who may be *invited to events such as openings (with their written consent).*

5.2 Individuals who provide the Association with personal information have:

- A right of access (through making a subject access request (SAR)) to a copy of the information comprised in their personal data;
- A right to object to processing that is likely to cause or is causing damage or distress;
- A right to prevent processing for direct marketing;
- A right to object to decisions being taken by automated means;
- A right in certain circumstances to have inaccurate personal data rectified, blocked, erased or destroyed; and
- A right to claim compensation for damages caused by a breach of the regulation.

Specific Personal Information Advice Sheet (Privacy Notices) have been prepared detailing our use of personal data (available from English Rural's website).

5.3 Exceptional circumstances in which personal information may be shared or used without the prior knowledge of the individual concerned include:

- For the prevention or detection of crime or the capture or prosecution of offenders;
- For the assessment or collection of tax or duty;
- To comply with the law or a court order;
- Where there is a clear health or safety risk;
- In connection with court proceedings or statutory action to enforce compliance with tenancy conditions;
- In an anonymised form for statistical research purposes.

5.4 There are special requirements of the GDPR in relation to "Sensitive Personal Information".

5.5 Sensitive Personal Information means personal data consisting of information about:

- The racial or ethnic origin of the data subject;
- Political opinions;
- Religious beliefs or other beliefs of a similar nature;
- Whether the individual is a member of a trade union (within the meaning of the Trade Union and Labour Relations (Consolidation) Act 1992);
- Physical or mental health or condition;
- Sexual life;
- Sexual orientation

5.6 Advice and authority will be sought from the relevant Executive Director if it is proposed to use any such Sensitive and Personal Information.

6. Data security

6.1 The Association takes the security of personal data seriously and has internal policies and controls in place to protect personal data against loss, accidental destruction, misuse or disclosure, and to ensure that data is not accessed, except by employees in the proper performance of their duties.

6.2 Where the Association engages third parties to process personal data on its behalf, such parties do so on the basis of written instructions, are under a duty of confidentiality and are obliged to implement appropriate technical and organisational measures to ensure the security of data.

7. Impact assessments

7.1 Some of the processing that the Association carries out may result in risks to privacy. Where processing would result in a high risk to data subjects rights and freedoms, the Association will carry out a data protection impact assessment (DPIA) to determine the necessity and proportionality of processing. This will include considering the purposes for which the activity is carried out, the risks and the measures that can be put in place to mitigate those risks.

8. Individual responsibilities

8.1 Everyone who works for, or on behalf of, the Association has some responsibility for ensuring data is collected, stored and handled appropriately, in line with this policy and the Association's Information Systems policies.

8.2 Individuals who have access to personal data are required:

- to access only data that they have authority to access and only for authorised purposes;
- not to disclose data except to individuals (whether inside or outside the Association) who have appropriate authorisation;
- to keep data secure (for example by complying with rules on access to premises, computer access, including password protection, locking computer screens when away from desk, and secure file storage and destruction including locking drawers and cabinets, not leaving documents on desk whilst unattended);
- not to remove personal data, or devices containing or that can be used to access personal data, from the Association's premises without prior authorisation and without adopting appropriate security measures (such as encryption or password protection) to secure the data and the device; and
- not to store personal data on local drives or on personal devices that are used for work purposes.
- to never transfer personal data outside the European Economic Area except in compliance with the law and with express authorisation from the Chief Executive
- to ask for help from the Business Support Officer if unsure about data protection or to highlight any areas where data protection or security can be further improved upon.

8.3 Failing to observe these requirements may amount to a disciplinary offence, which will be dealt with under the Association's disciplinary procedure. Significant or deliberate breaches of this policy, such as accessing personal data without authorisation or a legitimate reason to do so or concealing or destroying personal data without authorisation, may constitute gross misconduct and could lead to dismissal without notice.

9. Data breaches

9.1 The Association has measures in place to minimise and prevent data breaches from taking place. Should a breach of personal data occur the Association will take notes and keep evidence of that breach.

9.2 Any breach must be reported to the Chief Executive immediately.

9.3 If the Association discovers that there has been a breach of personal data that poses a risk to the rights and freedoms of data subjects, it will report it to the Information Commissioner within 72 hours of discovery.

10. Related Documents

10.1 This policy should be read alongside associated policies and procedures to support compliance with the Data Protection and Confidentiality Policy.

- Housing Management policies and procedures;
- Development procedures;
- Staff Handbook;
- Data Protection – Dealing with Data Subject Access Requests Procedure
- IT use Policy and Procedures.
- Personal Information Advice Notice also known as Privacy notices

10.2 Further reading

Further reading can be found on the ICO's website **https://ico.org.uk/for-organisations/guide-to-data-protection/**