



DATA PROTECTION (GDPR) POLICY

DATA PROTECTION GDPR POLICY

Contents

- 1.0 Statement**
- 2.0 The six GDPR Principles**
- 3.0 Definition of Terms**
- 4.0 Policy**
- 5.0 Privacy Notice**
- 6.0 Computerised and Manual Records**
- 7.0 Security**
- 8.0 Quality and Accuracy of Personal Data**
- 9.0 Consent or legal basis for processing personal data**
- 10.0 Conditions for processing special categories of data (Article 9 of the GDPR)**
- 11.0 Data Protection Impact Assessments**
- 12.0 Subject Access Requests (SARs) and the rights of Data Subjects**
- 13.0 Data Breaches**
- 14.0 Disclosure of Personal Data**
- 15.0 Users aged 13 and under**
- 16.0 Staff**
- 17.0 Equal Opportunities Implications**
- 18.0 Review**

DATA PROTECTION GDPR POLICY

1.0 Statement

- 1.1 The purpose of this policy is to set out the standards that Radcliffe Housing Society aims to achieve when handling related data, whether that is held electronically or manually. The policy applies to all data relating to residents, contractors, staff members, managers, vacancies and housing applicants.
- 1.2 The Data Protection Act 2018 allows individuals certain rights regarding information about them held by Radcliffe Housing Society (RHS) held in the ways set out above.

2.0 The six GDPR Principles

Personal data must be:

- 2.1 Principle 1 - Lawfulness, fairness and transparency
Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject
- 2.2 Principle 2 - Purpose limitation
Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes
- 2.3 Principle 3 – Data Minimisation
Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed
- 2.4 Principle 4 - Accuracy
Personal data shall be accurate and, where necessary, kept up to date
- 2.5 Principle 5 – Storage Limitation
Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed
- 2.6 Principle 6 – Integrity and Confidentiality
Personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures
- 2.7 Principle 7 - Accountability
The controller (RHS) shall be responsible for, and be able to demonstrate compliance with the GDPR

3.0 Definition of Terms

- GDPR Data Principles - the data protection principles set out the main responsibilities for organisations (See the seven main principles)
- Data - information recorded in manual or computerised form
- Data Controller (or Controller) – Radcliffe Housing Society Ltd

DATA PROTECTION GDPR POLICY

- Data Subject - an individual who is the subject of personal data
- Personal Data - information about an individual (the 'Data Subject') who can be identified from that information
- Special Categories - data regarding subject's racial or ethnic origins, political opinions, religious or other beliefs, TU membership, physical or mental health, sexual life and the commission or alleged commission of any criminal offences. Information on these topics can only be processed if certain conditions are met
- Relevant Filing System - any set of information structured by reference to individuals, or by reference to criteria relating to individuals, in such a way that particular information relating to a particular individual is readily accessible
- CEO (Data Protection Officer).

4.0 Policy

Personal data is confidential and will only be disclosed for registered purposes and in the course for staff carrying out their work. It will only be disclosed to others as detailed in the appropriate registration, to a Court under the direction of a Court order or for the purposes stated in 8, 9 and 13 of this policy. All staff are required to comply with the requirements of this Policy.

5.0 Privacy Notice

GDPR states that a privacy notice must be supplied to an individual at the time they provide their personal data to Radcliffe Housing Society. This should be written in plain language and easily accessible. We include our privacy notice on our website. It details:

- The use of customers' personal data and the safeguards in place
- How data will be processed for any additional purposes
- Customers' choices about the use of their data
- Who customers can contact about their personal data and how to access it
- How customers can withdraw their consent

6.0 Computerised and Manual Records

- 6.1 Computer and manual record systems and files will be designed to comply with the 7 GDPR principles and the Controller (RHS) must ensure that the processing of personal data complies with all seven principles.
- 6.2 We will maintain and update a document retention schedule to highlight personal data held in databases, the security of the information including access controls and the review processes.

7.0 Security

Security measures will be taken to ensure that there is no unauthorised access, alteration of, disclosure or destruction of, personal data and against accidental loss or destruction of personal data.

8.0 Quality and Accuracy of Personal Data

- 8.1 Radcliffe Housing Society undertakes to hold the minimum data necessary to enable it to perform its business. The data will be erased and securely destroyed once the need for us to hold it, has passed. This stipulation however will be overridden if there are specific requirements of the Chief Executive and our external auditors

DATA PROTECTION GDPR POLICY

who may require data to be held to facilitate the closing or audit of our accounts, where we have legal obligations to provide this.

- 8.2 Every effort will be made to ensure that the data is accurate and up to date and that inaccuracies are corrected without unnecessary delay. Therefore employees, residents, contractors and other data subjects are required to keep us informed of any changes in their personal circumstances, e.g. marital status, address, telephone numbers, next of kin etc.

9.0 Consent or legal basis for processing personal data

- 9.1 There are six main definitions of legal processing:

- **Consent** - Consent of the data subject
- **Contract** - Processing is necessary for the performance of a contract with the data subject or to take steps to enter into a contract
- **Legal Obligation** - Processing is necessary for compliance with a legal obligation
- **Vital Interests** - Processing is necessary to protect the vital interests of a data subject or another person
- **Public Task** - Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller
- **Legitimate Interests** - Necessary for the purposes of legitimate interests pursued by the controller or a third party, except where such interests are overridden by the interests, rights freedoms of the data subject

- 9.2 We will seek to ensure there is a legal basis for the processing of personal data, and this will be recorded appropriately. We will explain the reasons, and the legal basis (if there is one), for processing the personal data, and how the data will be used prior to processing it.

- 9.3 However, if consent is required to process personal data, including special category (sensitive personal) data, we will ensure that consent for the purpose in question is explicit. It will be clearly set out in all forms, including electronic versions, that consent is being sought. If consent is required for the processing of personal data for multiple purposes, then it will be obtained for each individual requirement.

10.0 Conditions for processing special categories of data (Article 9 of the GDPR)

- Explicit consent of the data subject and must meet the usual UK GDPR standard for consent
- Processing is necessary for carrying out obligations under employment, social security or social protection law, or a collective agreement
- Processing is necessary to protect the vital interests of a data subject or another individual where the data subject is physically or legally incapable of giving consent
- Processing carried out by a not-for-profit body with a political, philosophical, religious or trade union aim provided the processing relates only to member or former members (or those who have regular contact with it in connection

DATA PROTECTION GDPR POLICY

with those purposes) and provided there is not disclosure to a third party without consent

- Processing relates to personal data manifestly made public by the data subject
- Processing is necessary for the establishment, exercise or defence of legal claims of where courts are acting in their judicial capacity
- Processing is necessary for the establishment, exercise or defence of legal claims or where courts are acting in their judicial capacity
- Processing is necessary for reasons of substantial public interest on the basis of Union or Member State law which is proportionate to the aim pursued and which contains appropriate safeguards
- Processing is necessary for the purposes of preventative or occupational medicine, for assessing the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or management of health or social care systems and services on the basis of Union or Member State law or a contract with a health professional
- Processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of healthcare and of medicinal products or medical devices
- Processing is necessary for archiving purposes in the public interest, or scientific and historical research purposes or statistical purposes in accordance with Article 89(1).

10.1 Radcliffe Housing Society considers it justifiable under the Regulation to process personal data which we hold for human resources purposes when the:

- data subject has been informed that sensitive data about them will be held by Radcliffe Housing Society Ltd
- data subject has given their consent to sensitive data being held about them
- processing is necessary to fulfil a contract to which the data subject is party
- processing is necessary for legal purposes e.g. P.A.Y.E. and N.I.

11.0 Data Protection Impact Assessments

The GDPR contains a mandatory requirement for all new products and project developments that are likely to create “high risks” for the processing of individuals’ personal data for a Data Protection Impact Assessment (DPIA) to be incorporated into the development cycle. Radcliffe Housing Society will ensure that this requirement is built into the project appraisal process and that a set of screening questions are verified and answered by the developers.

12.0 Subject Access Requests (SARs) and the Rights of Data Subjects

12.1 Radcliffe Housing Society will make all reasonable efforts to ensure that data subjects are aware of the data which is kept about them, where it is kept and why it is kept. We will provide any individual who requests access in a reply stating whether we hold personal data about that individual and, if so, a written copy in clear language of the current data held. SARs can be made verbally or in writing, including by email or social media. SAR’s will be responded to within one calendar month

12.2 Information provided to the data subject will not identify another person in addition to the data subject, unless the other person has given written authorisation for the

DATA PROTECTION GDPR POLICY

disclosure to be made. Separate applications will be required for each of our entries in the Data Protection register.

- 12.3 Inaccuracies or omissions discovered as a result of an enquiry will be corrected without delay, and the individual will be sent an amended copy of the data without charge.
- 12.4 All employees are required to complete application forms and to notify the Chief Executive of any changes to their address, telephone number and next of kin details. This information will be held, with other details in connection with employment, in our internal records. An employee may inspect a file relating to him / her upon advance written request and in the presence of the Chief Executive.

13.0 Data Breaches

- 13.1 All breaches must be referred to the CEO immediately officers become aware of them. Reportable breaches need to be made to the Information Commissioner's Office within 72 hours of the organisation becoming aware of them. All breaches will be investigated by the CEO and any lessons learnt will be shared with all staff.
- 13.2 A breach of data security by any of our employees, could lead to disciplinary action, where an investigation give rise to a case of negligence.

14.0 Disclosure of Personal Data

- 14.1 Radcliffe Housing Society Ltd may disclose personal data if it is requested for any of the following purposes:
- the prevention or detection of crime
 - the apprehension or prosecution of offenders
 - the assessment or collection of any tax or duty

15.0 Users aged 13 and under

We will not knowingly collect or solicit personal information from anyone aged 13 or under or knowingly allow such persons to provide us with their personal information without parent or guardian consent. If any data is held for anyone aged 13 or under, we will get the permission of the parent or guardian. If we do not have the consent of the parent or guardian to process the personal data, we will delete that information.

16.0 Staff

- 16.1 We operate a clear desk policy to ensure all confidential materials are removed from staff workspaces and locked away when the items are not in use. This increases staff awareness about protecting sensitive information and establishes minimum requirements in maintaining a "clear desk" where any confidential information about our business is secured in locked areas and out of site.
- 16.2 It is the responsibility of staff members to ensure all confidential information in hardcopy or electronic form is secure.
- Computer terminals will be automatically locked if staff leave a computer unattended for a period of time. Computer terminals / workstations will be shut down at the end of the workday.

DATA PROTECTION GDPR POLICY

- All confidential information will be removed from desks
- Filing cabinets containing confidential information will be kept closed and locked when not in use or when unattended. Keys used for accessing confidential information storage will never be left visible.
- Portable computing devices such as laptops and tablets will be secured when not in use.
- On disposal of confidential documents, confidential disposal bins will be used
- Mass storage devices such as USB drives will be treated as sensitive and encrypted
- All printers will be cleared of papers as soon as they are printed

16.3 All staff will receive mandatory data protection training on induction and annually.

17.0 Equal Opportunities Implications

17.1 To monitor the effectiveness of our allocations, recruitment and selection policies, we will monitor applicants on grounds of their gender, marital status, colour, race, nationality, racial or ethnic origin, disability, membership or non-membership of a trade union, sexuality, age and religion.

17.2 To comply with the principles of the GDPR we will inform the data subject why this data is required and confirm it will be maintained confidentially, used appropriately and not imparted to non bona-fide requests. The collection of this data will inform any decision to amend our Housing Options Policy or recruitment and selection policies.

18.0 Review

This Policy will be reviewed from time to time to take account of changing legislation, organisational needs and trends in best practice. All data subjects (employees, contractors, residents etc) will be informed of any changes, no later than four weeks after effect.