Railway Housing Association

Policy Statement

Data Protection, Access to Information & Document Retention

1. Statement of Intent

1.1 The Association will comply with the Data Protection Act 2018, the General Data Protection Regulation 2016 and the Information Commissioner's Office guidance.

1.2 The Association recognises that the lawful treatment of personal information is essential to maintain the confidence of those with whom we deal with.

1.3 The Association is committed to ensuring that all appropriate technical and organisational measures are taken against unauthorised or unlawful processing of data and against accidental loss or destruction of, or damage to personal data**.**

1.4 This policy aims to protect and promote the rights of individuals and the Association, by identifying information that is to be treated as confidential, and outlining the procedures for collection, storage, handling and disclosure of such information.

1.5 The Association holds personal and confidential information about its prospective, current and former employees, board trustees, tenants and leaseholders and other members of their household, suppliers and contractors. This policy covers all records and information held by the Association in respect of these 'data subjects'.

1.6 This policy should be read in conjunction with the Association's Information Security, Internet Acceptable Use, Use of Tablet Devices and E-mail policies, which relate to computer held information.

1.7 The Association recognises that Public Authorities are required to provide certain information under the Freedom of Information Act 2000. Although the Association is not deemed to be a Public Authority within the terms of the Act, requests for information will be responded to where these are considered to be appropriate in the spirit of openness and transparency.

1.8 All employees and Board Trustees will treat all personal and special category information as confidential and comply with data protection legislation and this policy.

2. Definitions

2.1 Data protection legislation is designed to protect the individual and their personal data, which is held and processed on their behalf. The legislation defines the individual as the 'data subject' and their personal information as 'data'.

2.2 Data is any information that relates to a living person that can be used to directly or indirectly identify the person including a name, a unique identification number, a photograph, an email address, bank details, posts on social networking sites, medical information, a geographical location, or a computer IP address and any expression of opinion about the individual. It includes data that forms or is intended to form part of a filing system and also unstructured data in emails, spreadsheets and individual documents, manual and electronic records.

2.3 Special category data (previously known as sensitive personal data) is data relating to ethnic or racial origin, political opinion, religious beliefs or beliefs of a similar nature, trade union membership, genetic data, biometric data, physical or mental health, sexual life and orientation, offences, alleged offences, proceedings and sentencing arising from an offence.

2.4 Processing means anything done to data including collecting, recording, organising, structuring, storing, adapting, altering, retrieving, consulting, using, disclosing, disseminating, making available, combining, restricting, erasing, and destroying.

2.5 Encryption is a means of protecting electronically held data from unauthorised or unlawful processing by encoding it using a secret key/value. Only those users who are issued with the key/value are able to access the information.

2.6 Pseudonymisation is a privacy-enhancing technique where directly identifying data is held separately and securely from processed data to ensure that individuals cannot be identified. It is an important safeguard for processing personal data for scientific, historical and statistical purposes. GDPR recognises encryption and pseudonymisation as good practice.

2.7 A personal data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed.

3. Implementation

3.1 The Association will adhere to Article 5 of the General Data Protection Regulation 2016, which requires that the Association must be able to demonstrate that personal data shall be -

- Processed lawfully, fairly and in a transparent manner
- Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes
- Adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed
- Accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that is inaccurate,

having regard to the purposes for which it is processed, is erased or rectified without delay

- Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals

- 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.

3.2 The Association will not ask for information that is not necessary for business purposes.

3.3 The Association recognises that processing of personal data is only permitted if it meets one of the legal grounds for doing so, as specified by Article 6(1) of the GDPR –

- Consent has been given by the data subject

OR

Processing is necessary for –

- The performance of a contract with the data subject, or to take steps to enter into a contract;
- Compliance with a legal obligation;
- The protection of the vital interests of a data subject, or another person;
- The performance of a task carried out in the public interest, or in the exercise of official authority vested in the controller; or
- The purposes of legitimate interests by the data controller (the Association), or a third party, except where such interests are overridden by the interests, rights or freedoms of the data subject. (This condition is not available to processing carried out by public authorities in the performance of their tasks).

3.4 In order to lawfully process special category data, one of the legal grounds listed in 3.3 above AND a separate condition under Article 9 of the GDPR must also be identified –

- The data subject has given explicit consent for one of more specified purposes
- Obligations relating to employment, social security and social protection law
- Protecting the vital interests of the data subject or another person, where the data subject is physically or legally incapable of giving consent
- Legitimate activities of a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim
- The data has been made public by the data subject

- For the establishment, exercise or defence of legal claims
- Substantial public interest
- Preventive or occupational medicine, assessment of the working capacity of an employee, medical diagnosis, provision of health or social care
- Public health
- Archiving purposes in the public interest, scientific or historical research purposes of statistical purposes.

3.5 The Association is aware that consent cannot be a precondition of a contract or of signing up to a service, unless it is necessary for that service.

3.6 When consent is the legal basis for processing data, individuals will be offered genuine choice and control when asked for their consent. It will be a positive opt-in; pre-ticked boxes or any other method of consent by default will not be used. Consent forms will be clear and concise and make it clear that individuals have the right to withdraw consent and explain how to do this.

3.7 The legal basis for processing data will be identified and recorded. It will be explained in privacy notices and the data subject's rights will be explained clearly.

3.8 Some data may be used for a different purpose than the one for which it was originally collected. This is permitted if it is compatible with the original purpose taking into account –

- Any link between the original purpose and the purposes of the further processing
- The context in which the personal data was collected and the relationship between the data subject and data controller
- The nature of the data, in particular whether the new purpose involves the processing of special category data
- Possible consequences of further processing for the data subject
- The existence of appropriate safeguards such as pseudonymisation or encryption
- The reasonable expectations of the data subject. If the data subject would be surprised by the different purpose then it will be considered to be incompatible.

3.9 All personal and special category data that could identify a living person will be recorded on the Data Audit Register, which documents a clear description of the type of data involved, the categories of data subject to which it relates, where it came from, where it is stored, what security measures are in place, how and why it is processed, who it will be shared with and how long it will be retained. Staff will advise the Chief Executive of any personal information that is processed by any means other than that stated on the Register so that it can be updated.

3.10 Storage and Use of Information

3.10.1 Confidential information relating to prospective, current and former tenants and leaseholders and other members of their household, contractors and suppliers is held on the housing database, the main file server, the e-mail system and manual files in the relevant departments. (Refer to the

Information Security policy and E-Mail policy for information on computer held records).

3.10.2 Confidential information will only be accessible to staff and Board Trustees who need to know such information in order to carry out their duties.

3.10.3 Confidential information will be kept discreetly at all times, out of view of visitors to the office or other staff, board trustees and contractors who do not need access to the information in order to carry out their duties. Files will be suitably stored and will not be removed from the office unless absolutely necessary. If files are removed from the office then they will remain in the control of that member of staff or board trustee, kept secure and not visible to other persons.

3.10.4 Personal data will not be kept on computers or other media that do not belong to the Association unless the express consent of the Information Security Manager (currently the Finance & ICT Manager) has been given.

3.10.5 All portable computer equipment containing personal data being taken outside of the Association's offices will be kept securely and not left where it could be viewed or removed by unauthorised persons.

3.10.6 Members of staff, board trustees, applicants for housing, tenants, leaseholders and any other visitors will be offered a private place to discuss matters of a confidential nature.

3.10.7 Where there is a requirement to discuss confidential information internally, this will be done in private and only between members of staff or Board Trustees who have a legitimate right to access that information in order to carry out their duties

3.10.8 At the end of the working day, all confidential information will be moved out of view and wherever possible put away in desks and filing cabinets.

3.10.9 Visitors to the Association's offices will be accompanied around the building to ensure that they do not have unauthorised access to personal data.

3.10.10 When dealing with customers by telephone the Association will take steps to verify the identity of the individual before disclosing personal information.

3.10.11 Members of staff and Board Trustees will not discuss confidential information with third parties who have no need or right to know about the internal business of the Association.

3.10.12 The Association will give anonymity to tenants and leaseholders wherever practicable in reports to the Board of Trustees.

3.10.13 Confidential information relating to all prospective, current and former members of staff and Board Trustees is held securely by the Chief Executive. This information will be used for employment purposes and to assist in the running of the association. Senior managers may be given access to relevant information in order for them to effectively fulfil their staff management duties. Relevant confidential information will also be held securely by the Director of

Finance and the Finance & ICT Manager in order to administer the payroll and pension scheme.

3.10.14 Personal information relating to tenants and leaseholders will be used to: -

- assess and prioritise applications for housing
- enable the Association to fulfil its responsibilities as a landlord, for example, passing names and telephone numbers on to contractors so that arrangements can be made to carry out repairs
- tailor service delivery to meet individual's needs
- arrange care and support services for residents
- arrange other services such as concessionary TV licences
- comply with the Association's legal and regulatory obligations
- help prevent crime and deal with anti-social behaviour
- enable audit of services
- ensure that the Association's Equality and Diversity policy is being effectively implemented.

3.10.15 Equality information may be used to provide statistical information to organisations that regulate the Association. The information will be presented in a way that does not identify individuals.

3.10.16 Medical or health information will be used to assess applications for housing and adaptations; to assist residents in receiving appropriate care, support and assistance in an emergency; and to ensure that the Association manages sickness absence effectively and makes reasonable adjustments for members of staff and Board Trustees in accordance with the Equality Act 2010.

3.10.17 All applications for employment or accommodation will contain details of how the personal data will be used. Consent to disclose information to a third party will be obtained from each individual, who will be informed of the implications of giving consent.

3.10.18 Where a resident has personal difficulties that affect visitors or is known to be potentially violent, such information will not be provided to contractors in detail. Contractors will only receive the details necessary to safely complete their assigned work, for example, that they should not visit the resident alone.

3.10.19 The Association may use tracing agents for the collection of former tenant's and leasehold's arrears and other debts. Information will be passed to them as part of the debt recovery process.

3.10.20 Contracts with IT suppliers and any other companies that may hold personal data on our behalf will contain clauses limiting the use of the personal data and obliging the company to immediately inform us of any breach of security or loss/damage to personal data.

3.10.21 We may need to share data with other agencies such as the local authority, funding bodies and other voluntary agencies. The data subject will be made aware in most circumstances how and with whom their information will be shared. There are circumstances where data may be shared without the data subject's consent. These circumstances are limited to where the sharing is necessary for –

- Carrying out a legal duty
- Performing a contract that the Association has or will have in place with that particular data subject
- Protecting vital interests of a data subject or another person
- The pursuit legitimate interest of the Association or another person such as conducting any legal proceedings, obtaining legal advice or defending any legal rights or providing a confidential service except where that interest is overridden by the interest or fundamental rights of the data subject
- A task that is in the public interest, such as monitoring for equal opportunities purposes.

3.11 Vehicle Tracking Devices

3.11.1 Tracking devices may be fitted to vehicles hired, leased or owned by the Association in order to improve efficiency, safety and security. Data from tracking devices will be processed in accordance with the principles of data protection legislation and guidance.

3.11.2 Information collected may include –

- the location of the vehicle
- whether the vehicle is idling or not in use
- direction of travel
- journey distances and times, the speeds driven during journeys and the route taken
- the total time the vehicle has been driven over a day, week or longer.

3.11.3 The data may be collected in real time or as historical information.

3.11.4 The data may be used –

- to improve efficiency by monitoring routes and journey times to optimise route planning
- to summon assistance for the driver and/or vehicle in the event of an emergency
- to help recover the vehicle if it is stolen
- to provide information against third party claims or vehicle incidents
- to reduce the costs of vehicle insurance
- for disciplinary purposes if there is concern about the use of the vehicle or misconduct of a member of staff.

3.11.5 The tracking devices will only be monitored during working hours. If a device is used on a vehicle that is permitted for use outside of working hours then it will have a privacy setting or similar arrangement to enable the monitoring to be disabled.

3.11.6 The data from the tracking devices will only be accessible to those members of staff with a legitimate reason for doing so, usually the line manager and Director of the driver, in order to carry out their duties. However, in the event of an emergency it may be accessed by another senior member of staff or the Chief Executive's PA.

3.11.7 The data will be shared with the vehicle driver, their line manager and Director. It may also be shared with the senior management team, Chief Executive's PA and Board of Trustees when discussing staffing resources or disciplinary issues and with third parties such as the Police and insurers, but the data will be anonymised wherever practical so that individuals cannot be identified.

3.12 Close Circuit Television (CCTV)

3.12.1 The Association may wish to carry out surveillance of its offices and properties using CCTV apparatus, for the prevention, detection and investigation of crime. It may be used to gather evidence to apprehend and prosecute people who break the law, including those who are involved in anti-social behaviour such as harassment or graffiti.

3.12.2 All overt surveillance measures will comply with the data protection legislation, and in particular with the Information Commissioner's guide 'CCTV Data Protection Code of Practice'. This will include the use of appropriately sized signs informing of the presence of CCTV, the purpose (i.e. to prevent and detect crime) and contact details. Covert surveillance will comply with the Regulation of Investigatory Powers Act 2000 or the Investigatory Powers Act 2016 and will be authorised by an appropriate body such as the Police.

3.13 Images

3.13.1 Images may be captured during events we organise using photography, video or other medium and may be used on our website, newsletters, leaflets and other publicity material. We will inform everyone taking part in our activities that they may be filmed or photographed and ask for their written, informed, specific and granular consent before the start of the event.

3.14 Transfer of Information outside of the EU

3.14.1 Personal data will only be transferred outside of the EU in compliance with the conditions for transfer set out in Chapter V of the GDPR. Transfers will only be made where a) the European Commission has issued an adequacy decision stating that a country, territory, sectors or an international organisation ensures an adequate level of protection for personal data; or b) appropriate safeguards such as binding corporate rules or standard contractual clauses approved by the Information Commissioner's Office are in place; c) the data subject has explicitly consented to the transfer after being informed of the risks involved.

3.15 Disposal of Information

3.15.1 Personal information will be retained and disposed of in accordance with the Association's Document Retention Schedule.

3.15.2 Confidential items and papers that are no longer required will be disposed of by shredding or by an approved contractor who will supply a certificate of destruction of the items.

3.15.2 Anonymous information may be kept for statistical use, for example, equal opportunities.

3.16 Right to be informed

3.16.1 We will provide a privacy notice to data subjects, at the time that we collect their personal data from them. The privacy notice will be concise, transparent,

intelligible, easily accessible and in clear and plain language. It will inform data subjects how their data will be processed, how long it will be kept and who it may be shared with.

3.17 Right of access to information

3.17.1 All individuals have the right to see the personal information about them that is held by the Association.

3.17.2 Electronically held information includes word processing documents, emails, computer records, CCTV images, microfilmed documents, backed up files or data bases, faxes and information recorded in telephone logging systems.

3.17.3 Any request from a prospective, current or former tenant, leaseholder, supplier or contractor will be processed by the Director of Customer Services within the provisions of the GDPR and the Information Commissioner's Office guidance.

3.17.4 Any request from a prospective, current or former member of staff or Board Trustee will be dealt with by the Chief Executive within the provisions of the GDPR and the Information Commissioner's guidance.

3.17.5 Data may not be disclosed if it would adversely affect the rights and freedoms of others, for example if it contains personal data about a third party.

3.17.6 In accordance with the GDPR, any request for access to information may be refused if it is unfounded or excessive, in particular if it is repetitive. If a request is refused the Association will give the reasons for the refusal and inform the data subject of their right to make a complaint to the Information Commissioner's Office and to seek to enforce their right of access through the courts.

3.17.7 A fee may be charged if a request for access to information is excessive, particularly if it is repetitive. The amount charged will be based on the administrative cost of providing the information.

3.18 Incorrect Information

3.18.1 If an individual notifies the Association, verbally or in writing, that information held about them is incorrect and can provide factual evidence to support this, the information will be corrected, deleted or destroyed as appropriate. Where there is a disagreement, the individual's views will be recorded on file and attached to the disputed record. If incorrect personal information has been shared with a third party, we will inform them of the correction where possible. We will restrict the processing of the disputed data whilst considering its accuracy or the legitimate grounds for processing.

3.19 Right to erasure/to be forgotten

3.19.1 An individual may request deletion of their personal information if –

- It is no longer necessary for the purpose for which it was originally collected and processed
- The individual withdraws their consent
- The individual objects to the processing and there is no over-riding legitimate interest for continuing the processing
- The personal data was unlawfully processed
- The personal data has to be erased to comply with a legal obligation.

3.19.2 The right to erasure is not applicable if processing is necessary –

- to exercise the right of freedom of expression and information
- to comply with a legal obligation
- for the performance of a task carried out in the public interest or in the exercise of official authority
- for archiving purposes in the public interest, scientific research historical research or statistical purposes where erasure is likely to render impossible or seriously impair the achievement of that processing
- for the establishment, exercise or defence of legal claims.

3.19.3 We may refuse to comply with a request for erasure if it is manifestly unfounded or excessive, taking into account whether the request is repetitive in nature. If a request is refused the Association will give the reasons for the refusal and inform the data subject of their right to make a complaint to the Information Commissioner's Office and to seek to enforce their right of access through the courts.

3.20 Right to restrict processing

3.20.1 Individuals have the right to request that we restrict the processing of their personal data if -

- they contest the accuracy of their personal data and we are verifying the accuracy of the data
- the data has been unlawfully processed and they oppose erasure and request restriction instead
- we no longer need the personal data but they need us to keep it in order to establish, exercise or defend a legal claim
- they object to the processing of their data and we are considering whether our legitimate grounds override their rights.

3.20.2 If we have disclosed the personal data in question to third parties, we will inform them about the restriction on the processing of the personal data, unless it is impossible or involves disproportionate effort to do so.

3.20.3 We will not process the restricted data in any way, except to store it, unless -

- we have the individual's consent
- it is for the establishment, exercise or defence of legal claims
- it is for the protection of the rights of another person (natural or legal)
- it is for reasons of important public interest.

3.20.4 We may refuse to comply with a request to restrict processing if it is manifestly unfounded or excessive, taking into account whether the request is repetitive in nature. If a request is refused the Association will give the reasons for the refusal and inform the data subject of their right to make a complaint to the Information Commissioner's Office and to seek to enforce their right of access through the courts.

3.21 Right to data portability

3.21.1 The right to data portability allows individuals to obtain and reuse their personal data for their own purposes across different services. It allows them to move, copy or transfer personal data easily from one IT environment to another in a safe and secure way, without hindrance to usability.

3.21.2 The right to data portability only applies -

- to personal data an individual has provided to us;
- where the processing is based on the individual's consent or for the performance of a contract; and
- when processing is carried out by automated means.

3.21.3 If the personal data concerns more than one individual, we will take into consideration whether providing the information would prejudice the rights of any other individual.

3.21.4 We will provide the personal data in a structured, commonly used and machine readable form. If the individual requests it, we will transmit the data directly to another organisation, if this is technically feasible.

3.22 Right to object

3.22.1 Individuals have the right to object to -

- processing based on legitimate interests or the performance of a task in the public interest/exercise of official authority (including profiling);
- direct marketing (including profiling); and
- processing for purposes of scientific/historical research and statistics.

3.22.2 Individuals must have an objection on "grounds relating to his or her particular situation".

3.22.3 We will stop processing the personal data unless we can demonstrate compelling legitimate grounds for the processing, which override the interests, rights and freedoms of the individual; or the processing is for the establishment, exercise or defence of legal claims**.**

3.23 Right not to be subject to automated decision making and profiling

3.23.1 Individuals have the right not to be subject to a decision when it is based on automated processing; and it produces a legal effect or a similarly significant effect on the individual.

3.23.2 We will ensure that individuals are able to obtain human intervention; express their point of view; and obtain an explanation of the decision and challenge it.

3.23.3 The right does not apply if the decision is necessary for entering into or performance of a contract between us and the individual; is authorised by law, for example, for the purposes of fraud or tax evasion prevention; or based on explicit consent. The right does also not apply when a decision does not have a legal or similarly significant effect on someone.

3.24 Data Protection Impact Assessment (DPIA)

3.24.1 A DPIA, which identifies the specific risks to personal data as a result of processing activity, will be undertaken whenever there is a change in processes, technology, or new activity that is likely to result in a high risk to the rights and freedoms of individuals, for example, where processing includes systematic and extensive processing activities, large scale processing of special categories of data or personal data in relation to criminal convictions/offences, or large scale systematic monitoring of public areas i.e. CCTV.

3.24.2 The DPIA will include a description of the process and its nature, scope, context and purposes, an assessment of the necessity and proportionality of the processing in relation to the purpose, identification and assessment of the risk to individuals, identification of the measures in place to mitigate risk including security and to demonstrate compliance, and identification of any additional measures to mitigate residual risk**.**

4 Staff Training

4.1 All members of staff will be informed of this policy and it will form part of their Terms and Conditions of Employment together with the Information Security, Internet Acceptable Use, Use of Tablet Devices and E-Mail policies.

4.2 All staff with responsibility for handling confidential information will receive training on the requirements of data protection legislation and it will be included as part of their induction training programme.

5. Responsibility

5.1 The Chief Executive is responsible for the effective implementation of this policy and will ensure that the Data Audit Register is accurate and regularly updated.

5.2 The Director of Policy will act as the Data Protection Lead and provide guidance to other members of staff and board trustees on all aspects of data protection including the lawful basis for processing data, consent, privacy notices, retention periods, security, information breaches, and data subject rights.

5.3 All members of staff and Board Trustees are responsible for ensuring that they keep secure any personal data that they hold and do not disclose it to third parties unless in accordance with this policy.

5.4 Each member of staff and Board Trustee is responsible for informing their Director or the Chief Executive immediately if they are aware of a breach of confidentiality. A breach of confidentiality is a serious offence and may result in disciplinary action. Reports of suspected breaches of confidentiality will be dealt with in accordance with the Association's Whistle blowing policy.

5.5 The Chief Executive, or in their absence the relevant Director, will comply with statutory requirements to report to the Information Commissioner's Office any breaches of data protection that may result in a risk to the rights and freedoms of individuals and this includes events that, for example, may lead to financial loss, discrimination or loss of confidentiality. Where a breach is likely to result in a high risk to the rights and freedoms of individuals, we will also notify those concerned directly.

6. Review

6.1 This policy will be kept under review whilst guidance is still being issued on the GDPR and the Data Protection Act by the EU and the UK Information

Commissioner's Office; and thereafter reviewed every five years, or sooner should there be any change in statutory requirements.

April 2018

This policy can be made available on request in other languages, large type, Braille or in audio format.