Policy
Data Protection Policy

Date authorised	21 May 2019
Review date	2022

1.0 Purpose

Rosebery Housing Association (Rosebery) needs to gather and use certain information about individuals. These individuals can include customers, suppliers, business contacts, employees and other people that the organisation has a relationship with or may need to contact.

This Policy describes how this personal data shall be collected, handled and stored to meet the company's data protection standards and to comply with current legislation.

This Data Protection Policy ensures that Rosebery:

- Complies with obligations under the General Data Protection Regulation 2016 (GDPR) and the Data Protection Bill 2017 and any other relevant legislation,
- Follows good practice,
- Protects the rights of staff, customers and partners,
- Is open on how it stores and processes individuals' data,
- Protects itself from the risks of a personal data breach,
- Will seek guarantees over the security of information when personal data is transferred outside of the EU,
- Does not sell on personal information.

2.0 Scope

This Policy applies to all personal data in respect of which Rosebery is the data controller, regardless of its format, including all forms of digital data (including email), all forms of paper documents and all forms of archived data.

This policy applies to:

- All staff of Rosebery (permanent, casual and temporary).
- Rosebery Board members.
- All contractors, volunteers, suppliers and any other person working on behalf of or with Rosebery.

3.0 Policy

3.1 General staff guidelines

- All staff shall read and understand this Policy, including the requirement to protect data. Staff shall contact the Single Point of Contact (SPoC), Richard Deeks, in the first instance, if ever in doubt regarding the processing of personal data.
- The only people able to access personal data covered by this Policy shall be those that need it for their work.
- Personal data shall not be shared informally. When access to confidential information is required, employees can request it from their line managers.
- Rosebery shall provide training to all employees to help them understand their responsibilities when handling data.
- Employees shall keep all personal data secure.
- Passwords shall never be shared.
- Personal data shall not be disclosed to unauthorised individuals, either internally or externally.
- Personal data shall be regularly reviewed and updated if it is found to be out of date. If no longer required it shall be deleted.
- Employees shall request help from their line manager, our SPoC or the DPO if they are unsure about any aspect of data protection.
- Staff shall inform HR of any changes in their own personal data.
- Non-compliance to this Data Protection Policy by any relevant employee may result in disciplinary action being taken, in accordance with the Rosebery Disciplinary Policy.

3.2 Responsibilities

Everyone who works for or with Rosebery is responsible for ensuring that personal data is collected, stored and handled appropriately. The Board is ultimately responsible for ensuring that Rosebery meets its legal obligations.

The SPoC is supported by our nominated external data protection advisers and is responsible for:

- Keeping the Board updated about data protection responsibilities, risks and issues.
- Reviewing all data protection procedures and policies in line with an agreed schedule.
- Arranging data protection training for the individuals covered by this Policy.
- Advising and handling data protection questions from staff and anyone else covered by this policy.
- Ensuring that any request for personal information submitted by an individual is handled in accordance with Rosebery's Data Subject Rights processes.
- Checking and approving contracts or agreements with third parties that may handle Rosebery's sensitive data.
- Ensuring that Rosebery's data protection records are correct, valid and up to date.

Some of the responsibilities set out above may be delegated by the SPoC provided formal reporting and lines of communication are in place to ensure the SPoC retains adequate oversight of all related activities.

Rosebery appoints a Senior Information Risk Officer to be the strategic lead for data protection compliance. This Executive director (Corporate Resources Director) is the primary point of contact for the SPoC.

3.3 Risks

Unauthorised access to information and information processing facilities may cause breaches in confidentiality, integrity or availability leading to potential financial, legal or reputational loss and/or damage.

3.4 GDPR principles

3.4.1 Commitment and accountability

Rosebery processes personal data in accordance with the data protection principles defined in Article 5 of the GDPR, as described below, and demonstrates compliance with those principles, the requirements of data protection legislation and good practice by applying the policies and procedures set out in the Information Governance Framework. Anyone processing personal data shall comply with the following GDPR principles.

Data shall be:

1. Processed lawfully, fairly and in a transparent manner.
2. Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.
3. Adequate, relevant and limited to what is necessary.
4. Accurate and, where necessary, kept up to date.
5. Kept in a form which permits identification of data subjects for no longer than is necessary.
6. Processed in a manner that ensures appropriate security of the personal data.

3.4.2 Data protection by design and default and risk management

- Rosebery recognises that the processing of personal data poses a potential risk to the 'rights and freedoms' of data subjects whose information Rosebery collects and processes in accordance with the GDPR.
- Rosebery analyses, quantifies and documents risks in the Data Protection Risk Register. Each processing activity is recorded in the Register of Data Processing Activities and Lawful Reasons for Processing.
- Rosebery upholds the principles of data protection by design and default. Any new processing activities involving personal data are subject to a screening process that establishes whether a Data Protection Impact Assessment (DPIA) is required as specified in DPIA Procedure. The DPIA Procedure specifies that a full impact assessment shall be undertaken where there is a high risk to the rights and freedoms of data subjects.

Rosebery recognises that children merit special protection with regard to their personal data, as they may be less aware of how the processing may affect them and how to protect themselves and exercise their rights, particularly in relation to marketing and profiling. The interests of children are therefore given specific attention, including where parental consent is required and how this can be obtained.

3.4.3 Fair, lawful and transparent processing

Rosebery processes personal data in a fair, lawful and transparent manner.

Fair

- Rosebery understands fairness is about maximising the data subject's autonomy and choice about how and whether their personal data is used. For this to happen not only must the data subject not be misled to any extent about how their data will be used but that they are given clear and unbundled choices where processing is voluntary and that they are made fully aware of the risks, rules, safeguards and rights attached to that processing and how to exercise their rights in relation to such processing.

Lawful

- Rosebery ensures that no data collection activities are undertaken or commissioned without a lawful basis for processing having been identified and, in the case of special category personal data, a lawful basis for the data processing activities intended to be applied to the personal data.
- The relevant Information Asset Owner shall in all cases obtain the advice of the DPO on the lawful grounds for processing and ensure that processing complies with all relevant policies.

Transparent

- Through its Privacy Policy, Rosebery ensures no personal data is collected from a data subject without the information required by Article 13 of the GDPR being communicated to the data subject at the time the information is collected. Likewise, where personal data has not been collected direct from the data subject Rosebery ensures the information required by Article 14 of the GDPR is communicated to them in a timely manner and within one month at the latest.
- The Privacy Policy requires that the information communicated to data subjects is concise, easily accessible and easy to understand, that clear and plain language is used and, where appropriate, visualisation is used. Particular consideration is given to any

processing addressed to children or vulnerable adults so they can easily understand what is being communicated to them.

- The Privacy Policy also ensures that where personal data is collected direct from data subjects, transparency information is normally provided to them in the same way. Where the data being processed is sensitive or the intended use is unexpected or will have a significant effect on them or be shared in ways they would not normally expect, the transparency information will be actively brought to their attention.
- Rosebery ensures that its Register of Data Processing Activities and Lawful Reasons for Processing cross reference to the transparency information communicated to data subjects in connection with the relevant purpose and that these are maintained in our Privacy Notice for at least as long as the personal data to which they relate is retained.
- The DPO has an important role to play in promoting and advising on best practice.

3.5 Data processing purposes

- Information Asset Owners ensure personal data is not used for purposes other than that recorded in the Register of Data Processing Activities and Lawful Reasons for Processing.
- Where further processing of the personal data is compatible with the original purpose, the relevant Information Asset Owner shall ensure that the required transparency information is communicated to the data subject.
- Data shall always be processed in line with data subjects' rights. See 3.12.

3.6 Data matching and profiling

- As with any other processing, profiling or matching personal data with other information to evaluate certain aspects of a natural person must comply with each of the data protection principles. However, Rosebery recognises that profiling, whether or not it results in a legal or a similarly significant effect, poses significant risks for individuals and therefore requires additional measures to safeguard and protect individuals. This is particularly the case in relation to transparency, children and data protection by design.
- The rights of data subjects to object to profiling in its various forms are set out in Rosebery's Data Subject Rights Procedure.

3.7 Data adequacy and minimisation

- Rosebery uses a minimum of personal data in its processing activities and, at the same time, ensures personal data it collects is adequate for the identified purpose. The organisation undertakes periodic reviews to ensure that personal data remains relevant and adequate.
- Information Asset Owners ensure data collected is fit for purpose and no unnecessary, irrelevant or unjustifiable personal data is collected or created, either directly or indirectly, through the data processing activities they are responsible for and/or engage in. Information Asset Owners do this in respect of new or altered processing by following a risk-based approach to information governance and by undertaking a DPIA where appropriate.
- The DPO provides advice regarding the justification for personal data collected or created and ensures data collected is reviewed on a periodic basis.

3.8 Data quality

- Rosebery recognises personal data must be accurate and, where necessary, kept up to date and where personal data is inaccurate, having regard to the purposes for which it is processed, the data is erased or rectified without delay.
- Information Asset Owners ensure personal data for which they are responsible is accurate and, where necessary, up to date. Information Asset Owners ensure all employees are aware of the importance of accurate and up to date personal data and that they have written instructions on how this is to be achieved.
- Data subjects' rights to rectification and complaint are important ways in which the accuracy of personal data can be challenged and corrected. The Data Subject Rights Procedure provides for how claims for inaccuracy are dealt with and how any measures taken in consequence are recorded and reported.
- These measures include how processors and third parties are informed about inaccurate or out of date information that has been corrected.
- The Risk based Approach to Information Governance and Data Protection Impact Assessment (DPIA) Policy ensure issues of data quality and accuracy are taken into account when new processing is initiated.

3.9 Data retention

- Through its Retention Policy, Rosebery ensures it does not retain personal data for any longer than is necessary for legal or regulatory reasons or for its legitimate organisational purposes. Rosebery ensures timely and appropriate disposal at the end of the data's useful life through risk assessed measures such as erasure or anonymisation.
- Where personal data is to be transferred for long-term preservation (for example where it is of value for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes) Rosebery ensures that appropriate technical and organisational measures safeguard the rights and freedoms of the natural person.

3.10 Confidentiality, integrity and security

- Rosebery ensures any personal data it processes or commissions is processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and protection against accidental loss, destruction or damage, using appropriate technical or organisational measures.
- Any personal data breach that does occur is managed in accordance with the Data Breach Notification Policy including near miss breaches.
- All disclosures of personal data are controlled in accordance with the Data Sharing Policy.
- An Acceptable Use and IT Security Policy is maintained setting out specific policies in relation to keeping personal data secure, confidential, available and with integrity. This policy covers matters such as information security, human resource security, physical and environmental security, asset management and access control, communications security and cryptology, operations security and business continuity.
- The Head of IT formulates this policy and consults the DPO in regard to it. The DPO challenges the policy when appropriate and reports any concerns to the Executive directors.

3.11 Training and awareness

- Rosebery ensures employees and other workers are competent in and understand their data protection responsibilities assigned to them. Data Protection training is mandatory to all employees with annual refresh training to update on the fast moving changes to current legislation. All training is measured and reported in the organisation's CIPHR training records.

- The Head of Corporate Resources ensures the content of the Data Protection training programme are kept up to date and ensures employees and other workers are kept up to date through appropriate awareness briefings or communications.
- The SPoC ensures that employees are kept up to date and informed of any issues related to personal data.
- The SPoC and/or DPO maintains a list of relevant external bodies, the most important of which is The Information Commissioner's Office (ICO).
- The Rosebery Executive team promotes training and awareness and Rosebery Housing Association makes resources available to all employees.
- The SPoC and/or DPO demonstrates and communicates to employees the importance of data protection in their role and ensures that they understand how and why personal data is processed.
- The SPoC and/or DPO ensures that all security requirements related to data protection are demonstrated and communicated to employees to the same affect.
- Employees receive specific training on any information security requirements and procedures applicable to data protection and the data processing within their individual day-to-day roles and responsibilities, including reporting personal data breaches in compliance with the Data Breach Notification Policy.
- Employees receive specific training on dealing with complaints relating to data protection and processing personal data.
- The Head of HR retains records of the data protection training provided to employees.

3.12 Data subjects' rights

- Rosebery recognises the legal rights of the data subjects whose personal data it is processing, or intends to process, and ensures that appropriate information is provided to them advising them of their rights, and that policies and procedures are maintained to give effect to those rights.
- The Data Subject Rights Procedure sets out the division of responsibilities for responding to data subject rights requests.

  Rosebery recognises data subjects have the right:

  - To be provided with any and all information held about them, within one month and free of charge – see Data Subjects Rights Procedure.
  - To have their personal data erased, within one month and free of charge.

- To have incorrect or incomplete information rectified, within one month and free of charge. The information in question is then rectified and the data subject informed in writing, once the request has been completed.
- To have any or all processing of their personal data restricted. Processing is suspended until the processing in question has been resolved or the restriction has been lifted.
- To object to processing, including marketing, automated decisions and profiling. When such a request is received from a data subject Rosebery complies and ceases processing without delay.
- To have their personal data provided in a readable format and portable to another organisation. Rosebery responds to such requests by providing the requested information in a Comma Separated Variable (CSV) file format. Where it is not technically feasible to transfer the data to another organisation, Rosebery treats the request for data portability as it would a Data Subject Access Request, as described in the Data Subjects Rights Procedure.
- To lodge a complaint with the supervisory authority. All complaints are investigated following Rosebery's Complaints Procedure.
- To a fair judicial remedy if their complaint is not resolved or handled to a satisfactory standard. The DPO handles any such complaints including liaison with the supervisory authority or the applicable appointed court of law.
- To claim compensation from the controller, processor or supervisory authority for infringement of their rights. The DPO handles any such complaints, including liaison with the supervisory authority or the applicable appointed court of law.

- Rosebery recognises data subjects can:

  - Complain about how their personal data has been processed.
  - Complain about how their request for access to data has been handled.
  - Complain about how their complaint has been handled.
  - Appeal against any decision made following a complaint.

The SPoC and/or DPO handles any complaints in accordance with the Complaints Procedure.

Subject access requests from individuals shall be emailed to the DPO, contact details can be found under the 'Contact us' section on www.rosebery.org.uk

The Data Subjects Rights Procedure shall then be followed.

3.13 Children

- Rosebery takes special measures if it processes personal data relating to children under the age of 13, including the nature of privacy information provided and approach to information rights requests.
- Personal data relating to a child under the age of 13 is processed only with the consent of a parent or guardian.
- Rosebery demonstrates reasonable efforts have been made to verify the age of the child and establish the authenticity of the parental responsibility taking into consideration available technology.
- Rosebery Housing Association demonstrates that reasonable efforts have been made to establish the authenticity of the parental responsibility when withdrawing consent for the specified child, considering available technology.
- The processing activities that relied upon the consent are stopped in accordance with the relevant process. The DPO informs the relevant Information Asset Owner of this change so that processing is stopped.

3.14 Consent

- Rosebery interprets consent as it is defined in the GDPR and that any consent shall not be valid unless:

  - There is a genuine choice.
  - It has been explicitly and freely given and represents a specific, informed and unambiguous indication of the data subject's wishes that signifies agreement to the processing of personal data relating to them.
  - The consent was given through a statement made by the data subject or by a clear affirmative action undertaken by them.
  - Rosebery can demonstrate the data subject has been fully informed about the data processing to which they have consented and is able to prove it has obtained valid consent lawfully.
  - A mechanism is provided to data subjects to enable them to withdraw consent and which makes the withdrawal of consent as easy as it was to give, and that the data subject has been informed about how to exercise their right to withdraw consent.
  - Explicit consent is required for the processing of special categories of personal data.
  - Specific conditions apply to the validity of consent given by children in relation to information society services, with

requirements to obtain and verify parental consent for children below the age of 13.

- Rosebery recognises consent may be rendered invalid if any of the above points cannot be verified or if there is an imbalance of power between the data controller and the data subject.
- Rosebery recognises consent cannot be considered to be forever and applies a consent refresh procedure for every instance where consent is the lawful condition for processing.
- Rosebery provides a clear privacy notice wherever personal data is collected (to ensure consent is informed and the data subject is informed of their rights in relation to their personal data). Guidance for this is provided in the Privacy Notice.

Withdrawal of consent

- Rosebery ensures the withdrawal of consent by a data subject can be affected at any given time and is as easily done as giving consent.
- Rosebery demonstrates the data subject has withdrawn consent to the processing of his or her personal data.
- Where the processing had multiple purposes, Rosebery demonstrates withdrawal of consent for each purpose.
- The processing activities that relied upon the consent are stopped in accordance with the relevant process. The DPO informs the relevant Information Asset Owner of this change so that processing is stopped.

Withdrawal of parental consent

- Rosebery demonstrates the holder of parental responsibility over the specified child has withdrawn consent.
- Rosebery demonstrates that reasonable efforts have been made to establish the authenticity of the parental responsibility when withdrawing consent for the specified child, considering available technology.
- The processing activities that relied upon the consent are stopped in accordance with the relevant process. The DPO informs the relevant Information Asset Owner of this change so that processing is stopped.

3.15 Contractual arrangements with processors

- In accordance with the requirement in Article 28 of the GDPR, Rosebery ensures through the Processors Policy (controller to processor) that it only engages with processors who can provide a

sufficient guarantee of technical, physical and organisation security and are subject to a written contract, including specified terms.

- Prior to contracting with a new processor, Rosebery performs due diligence to ensure the proposed processor complies with the requirements of the GDPR. When a proposed processor has satisfied commercial obligations and has demonstrated compliance with the GDPR it is bound by a contract for the provision of services. The contract is filed centrally and recorded in the Register of Processors. Details of each processor are documented.
- The legally binding contract with the processor:

  - Sets out the subject matter and duration of the processing, the nature and purpose of the processing, the type of personal data, the categories of data subjects and the obligations and rights of Rosebery.
  - Sets out that the processor shall process personal data only under written instructions from Rosebery.
  - Sets out that, with regard to transfers of personal data to a third country or an international organisation, unless required to do so by European Union or Member State law to which the processor is subject, the processor shall inform Rosebery of any legal requirement before processing.
  - Ensures that employees authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.
  - Requires the processor to assist Rosebery in complying with data subjects' rights.
  - Specifies compliance with the legal requirements to notify Rosebery Housing Association of any security breaches or near miss breach without any undue delay.
  - Requires the processor to provide appropriate security for the personal data which it will process.
  - Enables regular audit of the security arrangements of the processor during the period in which the processor has access to the personal data.
  - Requires the processor to obtain Rosebery's permission to use further sub-processors to process the personal data.
  - Requires that contracts with sub-processors stipulate the sub-processor to comply with at least the same security and other provisions as the processor.
  - Requires that contracts with processors (which are flowed down to any sub-processors) specify that, when the contract is terminated, related personal data will either be erased or returned to Rosebery or to another organisation acting as a processor as specified by Rosebery Housing Association.

- Requires the processor makes available to Rosebery evidence of compliance with the contract.
- Rosebery is open and honest with data subjects about why their personal data is being processed by a processor and informs the data subject(s) accordingly, communicating this is via the Privacy Policy.
- Processing by an unauthorised processor, or any processing not covered by a valid processor contract is deemed to be a data breach and is investigated by the DPO;
- Any unauthorised processing in contravention of this policy which is knowingly or negligently performed or commissioned by an employee is dealt with under Rosebery's disciplinary policy and if it is also a criminal offence, the matter is reported as soon as possible to the appropriate authorities.
- When Rosebery receives a data subject rights request, such as a request to correct inaccurate personal data, Rosebery informs all processors processing the personal data.
- When processing of personal data by a processor is likely to cause a risk to the rights and freedoms of individuals, Rosebery conducts a DPIA to identify and address any privacy related risks.
- When Rosebery receives a data subject access request, Rosebery informs all processors that are processing the personal data and ensures the data is included in the response to the request.

3.16 Data sharing (controller to controller)

- When sharing personal data, Rosebery ensures it is shared in a safe and secure manner.
- Rosebery is open and honest with data subjects about why their personal data is being shared, what personal data is being shared, how it is shared and with whom. When Rosebery is obliged to share personal data for legal or regulatory reasons, it still informs the data subject accordingly. The principal method of communicating this is via the Privacy Policy.
- Any systematic or routine sharing of data between Rosebery and another party on a controller to controller basis is defined and detailed in a data sharing agreement before any data sharing commences. Such data sharing agreements articulate the roles of the data controllers and in particular avoid any circumstances where one of the parties could otherwise be construed as a processor, rather than a controller. These data sharing agreements are filed centrally.
- Rosebery only enters into data sharing activities where it is proven and documented the data sharing is fair and lawful.
- Data subjects are made aware of Rosebery's data sharing activities via the Privacy Policy which lists all routine data sharing activities.

- Sharing personal data with an unauthorised controller or sharing data in the absence of a valid data sharing agreement is deemed to be a data breach and is investigated by the SPoC and/or DPO in accordance with the Data Breach Notification Policy.
- Any breach of this Policy is dealt with under Rosebery's Disciplinary Policy and if it is also a criminal offence, the matter is reported as soon as possible to the appropriate authorities.
- When Rosebery receives a data subject rights request, such as a request to correct inaccurate personal data Rosebery informs any other controller with which the personal data has been shared.

3.17 Transfers of personal data to third countries

Where Rosebery has to transfer personal data to non-EEA countries (referred to in the GDPR as 'third countries') then this will always meet, as a minimum, the requirements of Chapter 5 of the GDPR. This details the following Articles:

Article 44 – General principle for transfers
Article 45 – Transfers of the basis of an adequacy decision
Article 46 – Transfers subject to appropriate safeguards
Article 47 – Binding corporate rules
Article 48 – Transfers of disclosures not authorised by Union Law
Article 49 – Derogations for specific situations
Article 50 – Intentional cooperation for the protection of personal data

3.18 Continuous improvement and internal audit

- Through its Audit Policy and Audit Procedure, Rosebery ensures there is a continuous cycle of internal audit of data protection risks. Priorities for audit are decided by the Internal Auditor in liaison with the DPO by reference to the Data Protection Risk Register and taking account of planned changes to systems and procedures.
- The audit programme explicitly includes any processing of high-risk personal data and addresses any non-conformance reports. Audit results and management reviews contribute to a culture of continuous improvement in data protection. The SPoC and/or DPO assists in this by analysing data protection complaints, security breaches, subject access requests and by horizon scanning technological and policy advances with colleagues across the organisation.