



Data Protection, Privacy and Information Security Policy

RS Group Pension Scheme

Prepared for: The Trustees of the RS Group Pension Scheme

Prepared by: Oliver Whelan

Date: 27 May 2025



Definitions

For the purposes of this Policy, “**Data Protection Laws**” is defined as, for the periods in which they are in force, the General Data Protection Regulation (Regulation (EU) 2016/679) as it applies in the UK (“**UK GDPR**”), the Data Protection Act 2018 (“**DPA**”), and any other applicable laws and regulations relating to data protection and privacy that amend, replace, or supplement the UK GDPR.

Contents

1. Introduction	3
2. Core Principles of this Policy	5
3. Trustee Practice to Ensure Security of Personal Data	17
4. Deletion and Destruction of Documents	20
5. Reporting Breaches	20
6. Compliance with this Policy	21



1. Introduction

In the ordinary course of administering and managing the RS Group Pension Scheme (the "**Scheme**") RS Pension Trustees Limited (the "**Trustee**") collects, holds, processes and transfers personal data relating to members of the Scheme ("**Members**") and other beneficiaries in receipt of benefits from the Scheme such as Members' dependants ("**Beneficiaries**").

The Trustee recognises the importance of establishing and operating a very high standard of data protection for personal data, as failure to do so can have serious legal implications and may, from 25 May 2018 for certain breaches of Data Protection Laws, result in the imposition of a fine of the higher of 4% of annual global turnover of the sponsoring employer and £17.5 million.

The Trustee is the data controller (as defined under Data Protection Laws) for any information that it collects from Members and Beneficiaries in connection with administering the Scheme.

This Data Protection, Privacy and Information Security Policy (the "**Policy**") relates to the handling and processing of all Members' and Beneficiaries' personal data, whether held manually or electronically, and sets out the minimum standards of conduct and procedure the Trustee expects for the handling of Members' personal data in compliance with the Data Protection Laws.

1.1 Who does this Policy apply to?

This Policy applies to the Trustee and to all directors of the Trustee. The Trustee will also have regard to this Policy in its dealings with its advisers, suppliers, the Scheme's sponsoring employer and other third parties including but not limited to other companies in the sponsoring employer's group.

Failure to adhere to this Policy may result in civil or criminal legal action being taken against the Trustee or against its individual directors by data protection authorities or by the individuals to whom the personal data relates.

1.2 What does the Policy relate to?

The processing of Member personal data. Processing means:

- carrying out any operation or set of operations on the data;
- collecting, recording or holding data; and
- use of the data which includes but is not limited to transferring, amending, consulting, sharing, storing, archiving and even destroying it.



1.2 What is Member personal data?

Any information relating to a Member or Beneficiary from which such Member or Beneficiary can be identified, directly or indirectly, or from which, with other information, they can be identified. These identifiers may include the Member's name, address, date of birth, an identification number such as a National Insurance number, health data, an online identifier or one or more factors specific to the physical, psychological, mental, economic, cultural or social identity of that Member.

It makes no difference where the data is held, e.g. whether it is in a computer database, on e-mails, or on paper in a filing system of such a type that the data is readily obtainable.

Review

This Policy will be reviewed at least annually or whenever there is a significant change in the Scheme which the Trustees consider requires this Policy to be reviewed.



2. Core Principles of this Policy

2.1 Data Protection Laws

It is essential that the Trustee and its individual directors:

- comply with this Policy;
- understand and observe any data protection laws applicable, including the Data Protection Laws, and
- ensure that Members' and Beneficiaries' personal data is handled with appropriate confidentiality and security.

2.2 Collection and Use of Personal Data

The term 'personal data' is any information relating to an identified or identifiable individual and an 'identifiable individual' is a living person who can be identified, directly or indirectly, in particular by reference to an identifier such as a name or address.

The Trustee collects personal data in many ways including but not limited to from Members and Beneficiaries (or their IFA) directly; from application forms completed by Members on joining the Scheme; from a Member's employer; from expression of wish forms completed by the Member; from information provided in relation to potential beneficiaries on the death of a Member, from track and trace services and from HMRC and other law enforcement agencies. The data is collected and processed for the purpose of:

- calculating and paying benefits;
- administering the Scheme which includes filing, storing and using Member personal data for general administrative purposes;
- managing the Scheme (as a whole and Members' membership of it) by the Trustee and any third party to whom the Trustee has delegated obligations arising in connection with Members' and Beneficiaries' benefits;
- carrying out obligations arising from any contracts entered into between Members and their employer and to provide Members with any information they request from the Trustee;
- analysis by the Trustee and, to the extent necessary, any other organisation required (such as the Trustee's external advisors, including legal advisers, and the Trustee's insurers or potential insurers);
- communicating with Members and Beneficiaries about their pension by mail, telephone, email, text or other electronic means;



- complying with the Trustee's auditing and/or reporting requirements;
- complying with legal and regulatory requirements or to protect the rights, property or safety of the Trustee, the Members and Beneficiaries, or others;
- complying with the Trustee's legal and regulatory obligations, resolving disputes and enforcing the Trustee's rights;
- implementing Court Orders and Pensions Ombudsman determinations and dealing with tax and other regulatory authorities;
- Specific liability management or risk transfers projects (e.g. enhanced transfer value exercises, longevity swaps, insurance transactions etc.).

2.3 Data Protection Principles

Both the DPA and the UK GDPR contain six thematic principles and an additional overriding principle that all data controllers must comply with when processing personal data.

Overview of the Data Protection Principles:

<p>1. Lawful, fair and transparent - personal data must be processed lawfully, fairly and in a transparent manner in relation to individuals.</p>	<p>2. Accuracy - personal data must be accurate and, where necessary, kept up to date. Every reasonable step must be taken to ensure that personal data that is inaccurate is erased or rectified without delay (having regard to the purposes for which it is processed).</p>
<p>3. Purpose limitation – personal data must be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.</p>	<p>4. Storage limitation - personal data must 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 is processed.</p>
<p>5. Data minimisation - personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which the data is processed.</p>	<p>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 of or damage to that data, using appropriate technical or organisational measures.</p>
<p style="text-align: center;">Overriding principle – Accountability</p> <p>Controllers are: (a) responsible for; and (b) required to be able to demonstrate compliance with; the data protection principles outlined above.</p>	



How will the Trustee apply the Data Protection Principles in practice?

This Policy has been drafted in line with the Data Protection Principles. The following sections describe how the Trustee will apply each of the Data Protection Principles in practice when processing personal data.

2.4 Principle One – Processing Personal Data Fairly, Transparently and Lawfully

Fair and Transparent Processing:

To process personal data fairly and transparently, the Trustee needs to make sure that it only processes personal data if the individual to whom it relates has been given certain information, including:

- who the data controller is (in this case the Trustee);
- the purposes for which the data is to be processed by the Trustee, and the lawful grounds for processing;
- in what circumstances, and to what types of organisations, data may be disclosed or transferred; and
- how long data will be kept and how it will be secured.

This will be set out in privacy notices which the Trustee makes available to Scheme Members, Beneficiaries and other individuals whose personal data the Trustee processes. The privacy notice for Scheme Members and Beneficiaries is available on the Scheme's website and available upon request from our administrators or the pensions manager.

An exception to this general rule applies in respect of individuals named in a Member's expression of wish form. The Trustee will keep such nominations confidential, even from the people nominated in them as communicated to Members. As a result, it would go against the Trustee's other legal duties if it issued a privacy notice to such nominated individuals. The Trustee will provide such individuals with the Scheme's privacy notice if they ultimately become a Beneficiary or become aware that they are being considered for benefits under the Scheme.

Lawful Grounds for Processing:

To process data lawfully, the Trustee must satisfy one or more of the lawful grounds for doing so for each processing activities that it undertakes. These lawful grounds are set out in the Data Protection Laws. The lawful grounds that are most relevant to the Trustee are summarised in Table A (for all personal data) and **in addition** to those, where the Trustee processes special categories of personal data, the Trustee must also satisfy one of the grounds set out in Table B.

In this context, 'special category data' refers to types of personal data that are considered more sensitive and therefore require additional protection under the Data Protection Laws.



These categories include (amongst others): health data, racial or ethnic origin and biometric data.

TABLE A: Lawful Grounds for Processing Personal Data:

The Trustee will take reasonable steps to ensure that any personal data is processed only if at least one of the lawful grounds set out below applies:

<p>Legal obligations</p>	<p>Processing is carried out to comply with a legal obligation placed on the Trustee (including both specific pensions legislation and common law obligations such as the Trustee's fiduciary duties). The Trustees are subject to legal obligations set out in legislation and common law (notably, trust law). Many of these legal obligations require the Trustees to process certain personal data.</p> <p>Such obligations include (but are not limited to) those found in trust law (i.e. the Trustee's fiduciary duties) and in statute (e.g. as set out under certain parts of the Pension Schemes Act 1993, the Pensions Act 1995, the Pensions Act 2004, and the Finance Act 2004 (and various other subsequent Finance Acts), and under the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017.</p> <p>This ground does not apply to any contractual obligations but it could apply to any data which was required by The Pensions Regulator under its statutory powers.</p> <p>It is essential for the Trustee to process the personal data relating to the Scheme for them to comply with their legal obligations.</p>
<p>Legitimate Interests</p>	<p>Processing is carried out to pursue the Trustee's legitimate interests (e.g. collecting personal data from Members in order to pay Scheme benefits) or the legitimate interests of a third party (e.g. if information is shared with the Scheme's employer for the purpose of helping the employer comply with their regulatory requirements).</p> <p>This condition only applies if the processing does not adversely affect the interests or fundamental rights and freedoms of the individual concerned. If there is a serious mismatch of competing interests between the Trustee and the individual, the individual's interests will have priority over business interests.</p> <p>The Trustee will carry out a legitimate interests balancing test as appropriate, for example where the Trustee's processing falls outside of the Trustee's 'core' / BAU activities.</p>
<p>Public task</p>	<p>Processing is necessary for the performance of a public task.</p>
<p>Consent</p>	<p>The individual has provided consent. In order to be valid, the individual's consent must be satisfy certain strict criteria. For more information on what constitutes valid consent, please see the</p>



	heading ' <i>When might consent or explicit consent be used?</i> ' below. Generally speaking, the Trustee will not rely on the consent of the data subjects as its lawful ground for processing personal data.
Contract	Processing is carried out to enter into a contract between the Trustee and the individual to perform such contract. As the Scheme is a trust-based arrangement, this ground will not normally provide a legal ground for processing personal data relating to Members.

TABLE B: Exemptions Permitting the Processing of Special Categories of Personal Data:

Employment and social security obligations*	Processing is necessary for the purposes of carrying out the Trustee's obligations in connection with employment, social security or social protection law (which are European-based references to pensions), or a collective agreement such as sick pay administration.
Publicly available information	Processing is carried out where it relates to the personal data manifestly made public by the data subject. This will only be used exceptionally by the Trustee.
Substantial public interest*	Processing is necessary for reasons of substantial public interest. This will only be used exceptionally by the Trustee, and the Trustee will identify the relevant part of the DPA.
Legal rights	Processing is necessary for the establishment, exercise or defence of legal claims. The Trustee will use this if necessary to exercise its legal rights or to defend itself from claims.
Explicit consent	Processing is carried out with the explicit consent of the data subject. For all of its core activities, the Trustee will not rely on the explicit consent of the data subjects as the Trustee <i>needs</i> to process personal data to comply with its legal obligations and could not comply with those obligations without processing personal data.

*[The Trustee has an Appropriate Policy Document in place, as required by the Data Protection Laws, for processing special categories of personal data under these grounds].

When might consent or explicit consent be used?

In exceptional circumstances only, where the data subject has a genuine choice about the Trustee's processing of their data, the Trustee may seek the Member's consent for the processing of personal data or explicit consent for the processing of special categories of personal data. Generally, the Trustee will not rely upon consent. This is because:



- individuals can withdraw consent at any time. In such cases, the Trustee may have to stop processing this data. This will take time to sort out and could complicate systems; and
- ICO guidance says that organisations should not rely on consent where any other condition is available.

2.5 Principle Two – Purpose Limitation

The Trustee will take appropriate steps to ensure that personal data is only processed if that processing is compliant under the original purpose for which this data was originally collected. Before processing a Member's personal data for another purpose, the Trustee will:

- ensure that the new purpose for the processing is compatible with the original purpose (e.g. scientific or historical research purposes, or statistical purposes);
- ensure that one of the legal grounds set out above is met; and
- notify the data subject of the new processing of their personal data.

The Trustee will apply the principle of purpose limitation by ensuring that the legal ground for processing is considered before beginning work on any new project or process that will use the personal data relating to the Scheme.

2.6 Principle Three - Data Minimisation

The Trustee only collects personal data that is relevant to the Trustee's legal duties and ensures that all data requested is adequate for, and limited to, those purposes. The Trustee will not collect any personal data which is not necessary for its stated purposes. The Trustee will work with its third party service providers to achieve data minimisation where appropriate and without compromising the Trustee's legal duties.

2.7 Principle Four – Accuracy

Personal data must be accurate and, where necessary, kept up to date. The Trustee will take appropriate steps to ensure the accuracy of personal data held on their systems by:

- receiving reports from time to time from the Scheme's administrators on the quality and accuracy of the personal data held by the Trustee;
- carrying out periodic data audits to check the accuracy of personal data held on its (or its third party service providers) systems;



- including a request for Members and Beneficiaries to update its details in communications issued by the Trustee from time to time; and
- requiring its third party administrators to amend or destroy inaccurate data promptly and to ensure that their systems have a single point of truth in respect of each identifiable beneficiary.

2.8 Principle Five – Storage Limitation

Personal data should not be kept longer than is necessary for the purpose for which it was obtained. This means that personal data should be destroyed or erased from systems when it is no longer required.

Given the long term nature of managing a pension scheme and the nature of the data held by the Trustee relating to Members, their dependants and Beneficiaries and to the possibility of claims being brought against the Trustee (which the Trustee ought reasonably be in a position to defend), the Trustee considers that it is generally necessary to keep personal data relating to the Scheme for the lifetime of the Scheme plus 15 years.

The Trustee will review the retention period above on a periodic basis and if there is a relevant material change affecting the Scheme. It will also consider from time to time whether there are any exceptions to the general retention approach outlined above.

2.9 Principle Six – Integrity and Confidentiality

Any disclosure of personal data must be subject to appropriate security safeguards and, depending on the nature of the personal data, confidentiality obligations.

The Trustee will ensure that the sharing of any personal data relating to the Scheme will be subject to appropriate security safeguards, including as appropriate

- where any personal data relating to the Scheme is kept in order to maintain accurate records but is no longer needed for the day to day running of the Scheme, the Trustee will consider the secure archiving of paper records and moving electronic files to secure offline storage;
- where personal data is no longer to be retained, the Trustee will comply with a safe disposal process for the destruction of hard copy and electronic files containing personal data;
- the Trustee will consider pseudonymising any personal data relating to the Scheme that is included in meeting packs, advice and emails by using scheme specific or case specific reference numbers rather than identifying details such as the member's full name, date of birth etc.;



- the Trustee will ensure that any sharing of personal data relating to the Scheme will be subject to appropriate security safeguards, such as email distribution controls so that emails that include or attach any personal data relating to the Scheme are only shared with those who need to have access to the information. The Trustee will require its third party service providers to take care when sending or replying to email messages with recipients in different organisations and will keep that under review;
- the Trustee will restrict access to documents that include personal data relating to the Scheme to those who need to have access. This may include (where appropriate):
 - password protection;
 - implementing access controls at a system level so that only specific individuals can access personal data relating to the Scheme; and
 - applying similar controls to the physical access to hard copy documents.

As most of the day to day processing of the personal data relating to the Scheme is carried out by third parties, the Trustee will also ensure that their contracts with those third parties contain clauses requiring the service provider to implement appropriate safeguards of technical and organisational security to protect against unauthorised or unlawful processing and against accidental loss, destruction of or damage to, personal data.

The Trustee will also liaise with the Scheme's key third party service providers to get sufficient comfort that:

- they have and will put in place appropriate data security measures;
- they have put and will keep in place appropriate technical and organisational measures that will ensure the ongoing confidentiality, integrity, availability and resilience of systems and services than involve the processing of any personal data relating to the Scheme;
- they have the ability to restore the availability and access any to personal data relating to the Scheme in a timely manner in the event of a physical or technical incident; and
- they have implemented a process for testing, assessing and evaluating the effectiveness of the Trustee's and third parties' technical and organisational measures for ensuring the security of the processing.

2.10 Overriding Principle – Accountability

Under the overarching principle of accountability, the Trustee, as a controller in respect of any personal data relating to the Scheme:

- is responsible for complying with the data protection principles; and
- is required to be able to demonstrate how they have complied with the data protection principles.



The Trustee will apply the principle of accountability by:

- maintaining a data protection policy which states how the Trustee complies with the data protection principles;
- with regard to special category data, where required, maintaining an Appropriate Policy Document;
- ensuring that each trustee receives training on data protection;
- ensuring that any decisions required to achieve compliance are made by appropriately trained and informed individuals and that records are kept of those decisions;
- retaining information relating to their audit of how their third party service providers give sufficient guarantees that they have implemented appropriate technical and organisational measures to ensure compliance with the UK GDPR and ensure the rights and freedoms of individuals;
- adding non-compliance with the Data Protection Laws to the risks faced by the Scheme in their risk register; and
- putting in place a periodic assessment of compliance with the Data Protection Laws and reporting on this at a trustee meeting.

2.11 Rights of the Individual

It is the Trustee's policy to respect the rights of Members and Beneficiaries and to provide them with reasonable access to data held.

The Trustee will provide Members and Beneficiaries with written information about the data it controls and how they should exercise their rights in relation to it through issuing them with a Fair Processing Notice. The Trustee issued an updated Fair Processing Notice to all Members and Beneficiaries on 23 May 2018 and will re-issue such notices where appropriate e.g. if it wishes to share personal data with a new third party. The Trustee acknowledges that it may also control personal data in relation to certain former Members of the Scheme (e.g. those who have transferred their benefits from the Scheme) but as it can no longer be certain that it holds up-to-date addresses for such persons, it has decided it would be disproportionate to send Fair Processing Notices to them.

At their written request, Members and Beneficiaries will be provided with a copy of their personal data held by the Trustee unless any such data can be legitimately withheld. Up until 25 May 2018, a fee of £10 was charged for this. After that date, the Trustee may request a fee only where appropriate in accordance with the Data Protection Laws, for example, if the



requests are manifestly unfounded or excessive, in particular because of their repetitive character.

If necessary the Member or Beneficiary making the request may be asked to prove his/her identity and may also be asked to provide information to enable the data in question to be located. The information should be provided as soon as is practicable and in any event within 30 days of the Member or Beneficiary making the request although this can be extended by a further 2 months if the request is particularly complex or a large number of requests are received by the Trustee.

Furthermore, at their written request, the information can be provided to Members and Beneficiaries in a way that makes it easy for a computer to read.

Members and Beneficiaries should be permitted to correct or update the information as necessary.

Members and Beneficiaries also have the right to ask the Trustee to delete or remove any personal data it holds in relation to them if:

- the personal data is no longer necessary for the administration and management of the Scheme;
- they have withdrawn their consent to processing and consent was the only legal basis on which the Trustee was entitled to process the data (e.g. potentially in relation to the processing of health data where the Trustee has no other lawful basis for processing such data);
- they have objected to the processing and there is no overriding legitimate interest for continuing the processing.

The Trustee can refuse a request from a Member or Beneficiary for his data to be deleted where the data is required to comply with a legal obligation e.g. in case of enquiries from HMRC or where it may be needed for the exercise or defence of legal claims. If the Trustee is unsure as to whether it should comply with such a request it should seek legal advice.

2.12 Special Categories of Personal Data

Special categories of personal data (formerly known as sensitive data) is information on a Member's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union memberships, physical or mental health, data concerning health or sex life and sexual orientation, genetic data and biometric data, criminal convictions and offences or related security measures where processing is not carried out under the control of official authority.

The collection and processing of special categories of personal data is very strictly regulated generally requiring the freely given, specific, informed and unambiguous consent of Members and Beneficiaries (unless processing is necessary to carry out the Trustee's legitimate interests, for example, to make a determination in connection with a Member or Beneficiary's eligibility for benefits payable under the Scheme and even then only where the Trustee has an enforceable data protection policy which sets out how such data is retained and erased).



It is the Trustee's policy to collect special categories of personal data only when absolutely necessary, for example, when considering an application for an ill-health early retirement pension or determining eligibility for a lump sum or spouse's pension following a Member's death.

Special categories of personal data must be made available to users only on a strict "need to know" basis, and managed with the highest practical level of security and confidentiality. For details of the Trustee's security and confidentiality measures, see section 2.13 below.

2.13 Disclosure of Personal Data

It is the Trustee's policy to ensure that personal data relating to Members and Beneficiaries is protected at all times, and it is the responsibility of all users of personal data to ensure that data is treated confidentially. The Trustee may share Members' and Beneficiaries' personal data with the Member's employer, other participating employers in the employer group, other companies in the employer's group, the scheme administrator and the Trustee's professional advisors and service providers to the extent that it is necessary for the management and administration of the benefits provided by the Scheme.

The Trustee may share Members and Beneficiaries' personal data with selected third parties including but not limited to:

- when specifically asked to do so by the Member or the Beneficiary e.g. to an independent financial adviser;
- in the event that the sponsoring employer sells or buys any business or assets, in which case the Trustee may disclose Members' or Beneficiaries' personal data to the prospective seller or buyer of such business or assets and their advisors;
- in the event that the Trustee considers de-risking or insuring any of the benefits provided by the Scheme in which case the Trustee may disclose Members' or Beneficiaries' personal data to prospective insurers and/or its or the sponsoring employer's advisers;
- if the Trustee is under a duty to disclose or share Members' and Beneficiaries' personal data in order to comply with any legal obligation or to protect the rights, property or safety of the Trustee, or others. This may include exchanging information with other companies and organisations for the purposes of fraud protection and credit risk reduction.
- When a member uses Pensions Dashboard data may be shared between the dashboards and data providers within the parameters of UK GDPR

The Trustee does not use Members and Beneficiaries' personal data for marketing purposes or transfer personal data to other organisations for the purpose of marketing their goods or services.



When the Trustee shares personal data with third parties, such third party will process Members or Beneficiaries' data as either a data controller or as the Trustee's data processor and this will depend on the purpose of the Trustee's sharing of the data.

Where personal data is disclosed to third parties who will be processing data controlled by the Trustee it must be done so in accordance with Data Protection Laws. In such circumstances:

- the Trustee must ensure that third parties are reliable, that they will keep data confidential, and that they have adequate technical and organisational security arrangements in place;
- a contract must be in place that binds the third party to the same obligations as apply to the Trustee, and under which the third party agrees to act only in accordance with instructions from the Trustee, and to take adequate technical and organisational security measures when processing personal data; and
- no more data should be provided than is necessary for the performance of the contract.

The personal data that the Trustee collects from Members and Beneficiaries may be transferred to, and stored at, a destination outside the EEA to the extent that it is necessary for the management and administration of the benefits provided by the Scheme. It may also be processed outside the EEA by the Trustee's advisers or suppliers. In compliance with the Data Protection Laws, should Members' and Beneficiaries' personal data be transferred to, and stored at, a destination outside the EEA the Trustee will take all steps reasonably necessary to ensure that such data is safeguarded through adequate means, such as ensuring that the recipient has entered into Standard Contractual Clauses approved by the European Commission

2.14 Data Security

The Trustee ensures that risk appropriate technical and organisational measures are in place to prevent unauthorised or unlawful processing and accidental loss, disclosure, destruction, damage or access to personal data, whether in the Trustee's possession or in the possession of third parties. Please see section 5 of the actions the Trustee takes to ensure the security of Members and Beneficiaries' personal data when in its possession.

The Trustee will also take reasonable steps to safeguard the accuracy and completeness of personal data, whether in the Trustee's possession or in the possession of third parties.

The Trustee ensures that data processors use, adopt and continue to comply with appropriate technical and organisational security measures. The Trustee ensures that:

- it is satisfied that data processors are clear about their responsibilities and that it has been provided with any written policies on the data processors' record keeping processes;



- it is clear about what data processors will, and will not, do for it and what information they need from it;
- it is satisfied that any information it needs from data processors is readily available so that it can meet its other legal and regulatory responsibilities;
- it informs data processors promptly about any changes in order that they can keep their records up to date;
- it is satisfied that it is kept informed of any problems data processors encounter with maintaining scheme records, or would be kept informed if any were to arise;
- any personal data sent by data processors to trustee directors is encrypted, anonymised or pseudonymised; and
- records are kept on the systems of the Scheme's administrator from time to time for as long as it takes to provide the pension and other benefits provided under the rules of the Scheme and for such period afterwards as necessary to comply with the Trustee's legal obligations, resolve disputes and enforce its rights.

Any data processors whose document destruction policies include the destruction of paper records once they have been converted to electronic images, must confirm that they have processes in place to ensure that any documentation destroyed does not include the Scheme's governing documentation, signed contracts, agreements, deeds and statutory declarations.

3. Trustee Practice to Ensure Security of Personal Data

The Trustee and its individual directors will comply with the following technical and organisational measures to aim to prevent the unauthorised or unlawful processing and accidental loss, disclosure, destruction, damage or access to personal data. The golden rule is to respect the privacy of the Members and the Beneficiaries to whom the data relates and to treat their data as highly confidential. This means that the Trustee and its individual directors will:

- comply with this Policy in all respects at all times;
- only record information which is necessary and not use it for purposes which have not been communicated to Members and Beneficiaries in the Trustee's Fair Processing Notice;
- not provide information unless it is certain the recipient is who they say they are and that they have a valid justification for receiving the data;



- provide only the data necessary to fulfil the purpose for which it is required by the recipient;
- not provide information over the telephone, fax, or in any other way, if the Trustee is not certain who will receive it. If in doubt, the Trustee will not give the information;
- ensure that the Trustee has explicit consent to process special category personal data or that it has another lawful basis for processing such data; and
- ensure that special category personal data is kept even more securely, with access strictly limited, and used only for the approved purpose. The Trustee will not collect such data unless it is essential to do so.

The only personal data relating to Members and Beneficiaries that the Trustee and its individual directors have access to:

- relates to individual Member cases (e.g. relating to death or ill-health cases) which the scheme administrator sends to the Trustee via its online portal PensionPal
- is contained within meeting papers issued by the scheme administrator as part of the electronic meeting pack sent via PensionPal.

Elementary housekeeping to ensure the security and confidentiality of such personal data is vital. In particular the Trustee's individual directors will:

- ensure that access to any personal data stored electronically is password protected, and keep passwords confidential;
- ensure that manual data and files are secure at all times, for example in a locked filing cabinet or locked drawer;
- not leave information unattended, whether paper records or unattended computer screens;
- ensure that personal data records are accurate and up-to-date, and that unnecessary and outdated records are deleted/destroyed;
- not print personal data if it is not essential to do so, and ensure that printouts are shredded and disposed of properly when no longer needed. In particular, the trustee director will ensure they do not keep any hard copies of individual Member cases or of any meeting packs at home and will shred or return any such material to the scheme administrator once the individual case has been considered or once they have reviewed and provided comments upon the minutes of any Trustee meeting;
- not forward or share any materials containing personal data except to the Trustee's advisers, other Trustee directors or to reply to the sender of the email;



- delete emails containing personal data (along with any attachments) as soon as they have been actioned;
- use a personal email address for Trustee business and access their emails via a securely protected mobile phone, tablet or personal computer.
- not allow anyone else access to their email account (including family members and other trustee directors although the trustee director may use the same email address for Trustee business as for other purposes;
- take appropriate measures to ensure the security of their mobile phone, tablet or personal computer as the case may be. In particular, each trustee director will ensure that such devices are password-protected and consider functionality to remotely wipe data if a device is lost or stolen;
- not store, upload or download any personal data from or to secure cloud services or run unofficial apps or use unauthorised services, such as Dropbox, Google Drive or similar;
- before accessing personal data from outside the EEA, consider whether such access is really necessary.

If any trustee director has any queries regarding how to ensure the security of their systems, they should speak to RS Group IT and Information Security Teams.



4. Deletion and Destruction of Documents

The Trustee will consider, on a regular basis, whether it is necessary to retain certain records. In doing so, the Trustee recognises that pensions are long-term investment vehicles and it is not uncommon for queries or disputes to arise in relation to Members' and Beneficiaries' benefits years after a Member has left the service of his employer or even after a pension has been put into payment. As a general rule, therefore, records relating to the calculation of Members' and Beneficiaries' benefits along with records relating to Members who have transferred their benefits out of the Scheme will be retained for 15 years following the winding-up of the Scheme. However, once a Member or Beneficiary's pension has been put into payment or a Member has transferred his pension out of the Scheme, the Trustee will take steps to ensure that access to such personal data is limited by arranging for it to be stored in an archive to which access is limited.

Each trustee director will ensure they do not keep any hard copies of personal data at home and will shred or return any such material to the scheme administrator once the individual case has been considered. Where hard copies of personal data are to be destroyed, the Trustee will always use a shredder or confidential waste bag.

If any trustee director has any doubt as to whether it is appropriate to delete or destroy a particular document, they will ask the Chair of Trustees who will decide the appropriate course of action.

5. Reporting Breaches

Breaches of this Policy, whether actual or suspected, must be reported by trustee directors to Head of Group Pensions or, in his absence, to a person designated by Head of Group Pensions to receive such reports, within 24 hours of becoming aware of a breach. The Head of Group Pensions will then investigate and consider what action should be taken, having obtained legal advice if required.

Where there has been a breach of Data Protection Laws the Head of Group Pensions must notify the Information Commissioner's Office without undue delay and where feasible no later than 72 hours after the relevant trustee director first became aware of the breach unless the breach is unlikely to result in a risk to the rights and freedoms of individuals. The Chair of Trustees should submit the report electronically to casework@ico.org.uk or on the Information Commissioner's Office website, and retain a copy of the notification.

Where a breach of Data Protection Laws is likely to result in a high risk to the rights and freedoms of individuals, the Trustee must also write to any affected individuals to notify them of the breach without undue delay. Should the Chair of Trustee have any doubt as to whether a particular breach is likely to result in a high risk to the rights and freedoms of individuals, they should seek legal advice.



6. Compliance with this Policy

The Trustee will review this Policy every year unless there are circumstances that merit an earlier review. It will monitor compliance with this Policy through its Risk Register.

As part of its Trustee training programme all trustee directors will be provided with data protection and security training within 6 months of appointment. Refresher training will also be provided to trustee directors as appropriate.

The Trustee is not required to have a Data Protection Officer under Data Protection Laws as it is not a public sector organisation, its core activities do not require the regular and systematic monitoring of data subjects on a large scale nor does its core activities require the processing of special category data and data relating to criminal convictions and offences. It has decided, therefore, not to appoint one.

Should a trustee director have any queries in relation to this Policy, they should contact Head of Group Pensions in the first instance.