[May 2025]

RS GROUP PENSION SCHEME

APPROPRIATE POLICY DOCUMENT FOR THE PROCESSING OF SPECIAL CATEGORY DATA AND CRIMINAL OFFENCE DATA

Who does this policy apply to?

RS Pension Trustees Limited is the Trustee of the RS Group Pension Scheme (the "**Trustee**", "**we**", "**our**", or "**us**"). The Trustee collects, holds and uses personal data to manage and operate the RS Group Pension Scheme (the "**Scheme**").

What data protection law applies to the Scheme?

The processing of personal data by the Trustee must be compliant with the UK General Data Protection Regulation (the **"UK GDPR"**) and the UK Data Protection Act 2018 ("**DPA**") as well as other related legislation which is applicable as implemented in the UK from time to time. Together, this legal framework is referred to in the rest of this document as the "**Data Protection Laws**".

What is the purpose of this document?

When we process special category data, or data about criminal convictions and offences, we need to do so in accordance with the requirements of Articles 9 and 10 of the UK GDPR and Schedule 1 of the DPA. Some of the Schedule 1 conditions for processing special category data and criminal offence data require us to have an Appropriate Policy Document ("**APD**") in place, setting out our procedures for securing compliance with Article 5 of the UK GDPR and policies regarding the retention and erasure of such personal data.

This APD explains our processing and satisfies the requirements of Schedule 1 of the DPA and, along with our suite of data protection policies and notices, aims to ensure that the processing of special category data and criminal offence data carried out by the Trustee is compliant with these requirements.

What is defined as special category data?

Special category data is defined at Article 9 (1) of the UK GDPR as personal data revealing:

- Racial or ethnic origin;
- Political opinions;
- Religious or philosophical beliefs;
- Genetic data;
- Biometric data for the purpose of uniquely identifying a natural person;
- Data concerning health; or
- Data concerning a natural person's sex life or sexual orientation.

What type of special category data and criminal offence data do we process?

The following types of special category data are likely to be relevant to the Scheme:

- Medical information
- Sexual orientation

The Trustee also processes criminal offence and conviction data.

Whose personal data does the Trustee process?

We process special category data and criminal offence data of:

- Members (or individuals who are or were connected to a member) of the Scheme;
- Beneficiaries; and
- Potential beneficiaries.

Why does the Trustee need to process special category data and criminal offence data?

Special category data is required so that the Trustee can (amongst other things):

- keep accurate and up to date records in relation to members and beneficiaries;
- provide benefits in accordance with the Scheme's governing documentation;
- consider properly and make informed decisions in relation to a member, beneficiary or potential beneficiary's eligibility for, and entitlement to, benefits such as death benefits, life cover and ill health benefits; and
- consider properly and make informed decisions in relation to a member, beneficiary or potential beneficiary's complaint whether under the Scheme's internal dispute resolution procedure or otherwise (to the extent this requires the disclosure of special category data or that such personal data has been provided to the Trustee by the member, beneficiary or potential beneficiary in question in relation to their complaint); and
- ensure that the Trustee does not pay benefits where a crime has been committed (typically fraud or identity theft) in order to obtain benefits to or where any other party is entitled to all or part of the benefits as a result of any individual's criminal activities (which bar the person claiming the benefits from entitlement).

LEGAL GROUNDS FOR PROCESSING PERSONAL DATA

The Trustee will typically rely on the following legal grounds to permit the processing of special category personal data:

(a) that the processing is necessary for the purposes of carrying out obligations and exercising specific rights of the Trustee or of members/beneficiaries in the field of employment and social security and social protection law; or

(b) that the processing is necessary for reasons of substantial public interest – occupational health schemes.

The Trustee relies on the legal ground of substantial public interest, preventing or detecting unlawful acts to process criminal offence data.

Employment, social security or social protection law

When the Trustee processes special category personal data, the processing is considered necessary for the Trustee to perform or exercise obligations or rights which are imposed or conferred by law on

the Trustee or member/beneficiary in connection with employment, social security[1] or social protection[2]. In this regard, the Trustee is subject to trusts law which imposes obligations on the Trustee to manage the Scheme and its assets which is ultimately for the purpose of and in connection with social security and the social protection of the members.

Substantial public interest – occupational pension schemes

The DPA contains a public interest exemption that applies to occupational pension schemes. This exemption is, however, of very limited practical use because the conditions require that the processing:

- is necessary for the purpose of making a determination in connection with eligibility for, or benefits payable under, the Scheme;
- is of data concerning health which relates to a data subject who is the parent, grandparent, great-grandparent or sibling of a member of the Scheme;
- is not carried out for the purposes of measures or decision with respect to the data subject; and
- can reasonably be carried out without the consent of the data subject (the requirements of which are as set out in paragraph 21(2) of Part 2, Schedule 1 of the DPA).

Substantial public interest – preventing or detecting unlawful acts

Like any organisation, but particularly in light of the fiduciary duties to which Trustees are subject, the Trustee has to take measures to avoid paying benefits to anyone other than the person who is entitled to receive them. The Trustee uses available checklists, techniques and processes to prevent and detect crimes like fraud and identity theft, which require use of personal data and, if criminal activity is detected, could result in the Trustee processing information about criminal offences or convictions.

PROCEDURES FOR ENSURING COMPLIANCE WITH THE GDPR PRINCIPLES

Accountability principle

We have put in place appropriate technical and organisational measures to meet the requirements of accountability. These include:

- 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 the 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;

[1] Social security includes (but is not limited to) old-age benefits, survivors' benefits, invalidity benefits, sickness benefits.

[2] Social protection includes interventions intended to relieve households and individuals of the burden of a defined risk, provided that neither a simultaneous reciprocal arrangement nor an individual arrangement is involved. Risks relevant to Trustees that may give rise to social protection are sickness old age and survivorship. .

- retaining information relating to their audit of how the Trustee's 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.

Principle (a): lawfulness, fairness and transparency

Processing personal data must be lawful, fair and transparent. It is only lawful if and to the extent it is based on law and either the data subject has given consent for the processing, or the processing meets at least one of the conditions in Schedule 1 of the DPA. We have documented above which of the conditions in Schedule 1 of the DPA apply to our processing of special category data and criminal offence data.

In relation to the fair processing and transparency principle, the Trustee has in place a privacy notice which informs data subjects of the categories of data processed by the Trustee in administering the Scheme. This privacy notice is reviewed on a regular basis by the Trustees. Any amendment to a version in place must be approved by the Trustees.

Principle (b): purpose limitation

The processing of members' special category data is allowed only for the purposes set out above to process data under the employment, social security or social protection law or the substantial public interest legal ground. The use of data subjects' special category data for a different purpose must be expressly approved by the Trustee, who will also be responsible for approving any consent forms used for this purpose, where appropriate.

The Trustee will not process personal data for purposes incompatible with the original purpose for which it was collected.

Principle (c): data minimisation

The Trustee will only use the data that is necessary to achieve each of the purposes for which special category data and criminal offence data is used. As a general rule, only the data detailed in this APD should be used for the legal grounds set out in this APD.

The use of other data classified as special category data must be approved by the Trustee, who will take steps to update this document accordingly if appropriate. This document will also be reviewed to ensure that the data listed in this section is still necessary to achieve the purposes for which special category data and criminal offence data is processed.

Principle (d): accuracy

Personal data must be accurate and kept up to date. Information which is incorrect or inaccurate is misleading and steps should therefore be taken to check the accuracy of any personal data at the point of collection and at intervals afterwards. Inaccurate or out of date personal data should be destroyed or erased from the Trustee's systems.

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.

Principle (e): storage limitation, including retention and erasure policies

The Trustee has considered what retention period is appropriate for the use of each of the special category data and criminal offence data detailed in this APD. Given the long term nature of managing a pension scheme and the nature of the data held by the Trustees relating to members, their dependants and beneficiaries and to the possibility of claims being brought against the Trustee (which the Trustee ought reasonably to be in a position to defend), the Trustee considers that it is generally necessary to keep such personal data for the lifetime of the Scheme plus 15 years. Once a retention period has expired, the data must be securely deleted.

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.

Our service providers (and former service providers) may also have similar valid grounds to keep your personal information for such long periods.

Principle (f): integrity and confidentiality (security)

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 any sharing of the Scheme's personal data 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 Scheme's personal data;

- where appropriate, the Trustee will consider Pseudonymising any of the Scheme's personal data 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.

- 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 that involve the processing of the Scheme's personal data;

- they have the ability to restore the availability and access to the Scheme's personal data 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.

APD review

This policy will be retained for the lifetime of the Scheme and reviewed periodically to assess the need for changes.

Version dated: [May 2025]