Scottish Rail Holdings Limited

Personal Data Retention Policy

Release Certificate	
Status of this Document:	Interim
Document Version:	1.0
Release Date:	19/05/2025

Document Control

Title:	SRH Personal Data Retention Policy
Reference:	SRH / Information & Data / 6.5
Version:	1.0
Release Date:	19/05/2025
Author:	Neil Amner, General Counsel
Total Pages:	17 including preliminaries & Appendix
Classification:	Official
Distribution:	SRH Internal
Disclaimer:	This document is uncontrolled when printed.

Document Approval

Approved By:	SRH General Counsel, acting under December 2024 Board direction	Interim edition pending Board review later in 2025.

Revision History

Version	Date	Issued By	Status	Comments
0.1	16/01/2025	DPO	Draft	First draft with DPO revisions.
0.2	16/01/2025	Administrator	Draft	Second formatted for approval by General Counsel.
1.0	19/05/2025	General Counsel	Interim	Interim Edition.
1.0	19/05/2025	Administrator	Published	Published on SRH Intranet.

Table of Contents

SRH Personal Data Retention Policy

1 Aim of this policy

1.1 This Personal Data Retention Policy sets out Scottish Rail Holdings Limited ("**we**", "**our**", "**us**", "**SRH**") will comply with the retention requirements of the UK GDPR and Data Protection Act 2018.

1.2 SRH has defined retention schedules for the Personal Data it processes. These are recorded in the Data Retention Schedule below ("**Data Retention Schedule**") which seeks to capture all of the personal data processed by SRH in its capacity as a Data Controller.

1.3 There are legal and regulatory requirements for SRH to retain certain Personal Data for a specified amount of time and we also retain some data for operational purposes.

1.4 We do not, however, need to retain all Personal Data indefinitely and retaining data for longer than necessary can expose us to risk as well as imposing a cost to our business. To mitigate such risks, all SRH Personnel must comply with the retention periods listed in the Data Retention Schedule.

2 Scope

This Policy covers all personal data that we hold or have control over. This includes electronic and physical copies of personal data.

3 Definitions

Controller: the person or organisation that determines when, why and how to process Personal Data. It is responsible for establishing practices and policies in line with the UK GDPR. We are the Controller of all Personal Data relating to our SRH Personnel and Personal Data used in our business for our own commercial purposes.

Criminal Convictions Data: personal data relating to criminal convictions and offences, including personal data relating to criminal allegations and proceedings.

Data Subject: a living, identified or identifiable individual about whom we hold Personal Data. Data Subjects may be nationals or residents of any country and may have legal rights regarding their Personal Data.

Data Protection Officer (or 'DPO'): SRH's DPO, contactable by email to dpo@railholdings.scot At the time of publication of V1.0 of this policy, we have outsourced this role to Thorntons Law LLP, with Loretta Maxfield, Partner being our point of contact (and who can be contacted on DPO@railholdings.scot).

General Counsel (or 'GC'): SRH's GC, contactable on GC@railholdings.scot . At the time of publication of V1.0 of this policy, the GC is Neil Amner.

UK GDPR: the retained EU law version of the General Data Protection Regulation ((EU) 2016/679) as defined in the Data Protection Act 2018. Personal Data is subject to the legal safeguards specified in the UK GDPR.

Personal Data: any information identifying a Data Subject or information relating to a Data Subject that we can identify (directly or indirectly) from that data alone or in combination with other identifiers we possess or can reasonably access. Personal Data includes Special Categories of Personal Data and Pseudonymised Personal Data but excludes anonymous data or data that has had the identity of an individual permanently removed. Personal data can be factual (for example, a name, email address, location or date of birth) or an opinion about that person's actions or behaviour.

Processing or Process: any activity that involves the use of Personal Data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data including organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transmitting or transferring Personal Data to third parties.

Pseudonymisation or Pseudonymised: replacing information that directly or indirectly identifies an individual with one or more artificial identifiers or pseudonyms so that the person to whom the data relates cannot be identified without the use of additional information which is meant to be kept separately and secure.

Related Policies: SRH's policies, operating procedures or processes related to this Data Protection Policy and designed to protect Personal Data, available on the SRH intranet or from the GC, failing which the DPO.

Special Categories of Personal Data: information revealing racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health conditions, sexual life, sexual orientation, biometric or genetic data.

SRH Personnel: everyone working for SRH, including all employees, consultants, secondees, contractors and agency staff.

4 Who does this policy apply to?

This Policy applies to all SRH Personnel

5 Does this policy form part of my contract?

This policy does not form part of your contract except to the extent that it imposes obligations on you.

6 Data Protection Principles

6.1 SRH is committed to the processing of personal data only where there is a lawful basis to do so and processing will be conducted in accordance with the data protection principles in applicable data protection legislation. More information on these principles can be found in the Data Protection Policy.

6.2 Under the storage limitation principle of data protection law, personal data must not be kept in an identifiable form for longer than is necessary for the purposes for which

the data is processed. We must take all reasonable steps to destroy or erase from our systems all personal data that we no longer require. This includes requiring third parties to delete that data where applicable.

7 Guiding Principles

Through this Policy, and our data retention practices, we aim to meet the following commitments:

- We comply with legal and regulatory requirements to retain Personal Data.
- We comply with our data protection obligations, in particular to keep Personal Data no longer than is necessary for the purposes for which it is processed (storage limitation principle).
- We handle, store and dispose of Personal Data responsibly and securely.
- We create and retain data where we need this to operate our business effectively, but we do not create or retain data without good reason.
- We allocate appropriate resources, roles and responsibilities to data retention.
- We regularly remind employees of their data retention responsibilities.
- We monitor and audit compliance with this Policy and update this Policy when required.

8 Retention Periods

8.1 As explained above, data protection laws require us to retain Personal Data for no longer than is necessary for the purposes for which it is processed (principle of storage limitation). Where data is listed in the Data Retention Schedule, we have taken into account the principle of storage limitation and balanced this against our requirements to retain the data.

8.2 If any Personal Data processed by you is not listed in the Data Retention Schedule, and you think there has been an omission in the Data Retention Schedule, or if you are unsure, please contact the GC, failing which the DPO.

9 Storage and Disposal of Personal Data

9.1 Personal Data must be stored in a safe, secure, and accessible manner.

9.2 Each Directorate is responsible for the continuing process of identifying the Personal Data it processes that has met its required retention period and supervising its destruction.

9.3 The destruction of confidential, financial, and employee-related hard copy data must be conducted by shredding if possible. The destruction of electronic data must be co-ordinated by each Directorate with technical support as necessary.

10 Compliance

10.1 You must read, understand and comply with this Personal Data Retention Policy and attend training on its requirements.

10.2 Your compliance with this Personal Data Retention Policy is mandatory.

10.3 Related Policies are available to help you interpret and act in accordance with this Personal Data Retention Policy. You must also comply with all those Related Policies.

10.4 Any breach of this Personal Data Retention Policy may result in disciplinary action.

10.5 If you become aware of any failure to comply with this policy , whether by yourself or other SRH Personnel, then report it as soon as you can to the General Counsel or otherwise the DPO.

10.6 Where a breach of this procedure is reported or discovered, SRH will undertake a detailed investigation involving the examination and disclosure of applicable records to those nominated to undertake the investigation.

10.7 If you have any questions regarding this Policy, please contact the GC, or the DPO.

11 Responsibilities

11.1 **SRH Board** are responsible for approval and formal support of this Personal Data Retention Policy and Related Policies (together "**the Policies**")

11.2 **SRH General Counsel** is responsible for:

- Drafting, development and maintenance of the Policies;
- Taking proactive steps to engage users with the Policies and assist in understanding the requirements outlined in the Policies;
- Taking proactive steps to reinforce compliance with the Policies;
- Reviewing instances of non-compliance with any of the Policies.

11.3 **DPO** is responsible for advising on Data Protection issues and for reviewing the Policies at regular intervals.

11.4 **SRH Executive Team** are responsible for ensuring all SRH Personnel comply with the Policies and the need to implement appropriate practices, processes, controls and training to ensure that compliance.

11.5 **All SRH Personnel** are responsible for:

- your own compliance with the requirements of the Policies; and

- reporting of instances of non-compliance to the General Counsel, or otherwise the DPO, as soon as possible

12 Review and amendment

12.1 This policy will be reviewed every two years or sooner if there is a change in the applicable law.

12.2 SRH may amend this policy at any time and may vary it as appropriate to a particular case.

13 Related documents

The following SRH policies, and further policies and procedures referred to in them, are relevant to the interpretation and application of this policy:

- Data Protection Policy
- Sharing of Personal Data with Third Parties Procedure
- Appropriate Policy Document;
- Employee Privacy Notice;
- Applicant Privacy Notice;
- DPIA Procedure;
- DPIA Template Form;
- Handling Data Subject Requests Procedure;
- Personal Data Breach Procedure and Form;
- Records Management Policy;
- Freedom of Information Policy;
- Staff Code of Conduct;
- Disciplinary Policy; and
- Whistleblowing Policy.

Those policies are available on the SRH intranet.

14 Appendix

The Appendix contains the Data Retention Schedule.

Data Retention Schedule

SRH establishes retention or destruction schedules or procedures for specific categories of data. This is done to ensure legal compliance (for example with our data protection obligations) and accomplish other objectives, such as protecting intellectual property and controlling costs.

SRH Personnel should comply with the retention periods listed in the record retention schedule below, in accordance with the SRH Personal Data Retention Policy (above).

If you hold data not listed below, please refer to the SRH Personal Data Retention Policy. If you still consider your data should be listed, if you become aware of any changes that may affect the periods listed below or if you have any other questions about this Data Retention Schedule, please contact the GC, failing which the DPO.

TYPE OF DATA	RETENTION PERIOD
Job Applicants	
• Completed online application forms or CVs. • Equal opportunities monitoring forms. • Assessment exercises or tests. • Notes from interviews and short-listing exercises.	12 months after notifying candidates of the outcome of the recruitment exercise.
• Pre-employment verification of details provided by the successful candidate. For example, checking qualifications and taking up references. (These may be transferred to a successful candidate's employment file.) • Criminal records checks. (These may be transferred to a successful candidate's employment file if they are relevant to the ongoing relationship.)	Details will only be retained if relevant to employment or where a legal obligation exists to retain it (in which case will be retained either until conviction spent, or in line with the legal obligation, up to the maximum of 7 years after employment ends).
Immigration Checks	3 years after the termination of employment.
Employment Contracts	
• Written particulars of employment. • Contracts of employment or other contracts. • Documented changes to terms and conditions.	While employment continues and for 7 years after the contract ends.
Collective Agreements	

• Collective workforce agreements and past agreements that could affect present employees.	Any copy of a relevant collective agreement retained on an employee's record will remain while employment continues and for 7 years after employment ends.
Payroll and Wage Records	
• Payroll and wage records • Details on overtime. • Expenses. • Benefits in kind. • Redundancy/Disturbance Allowance. • Overpayments/timesheets/pension contributions/any other pay records or pay related forms.	7 years after employment ends.
• Current bank details	Bank details will be deleted as soon after the end of employment as possible once final payments have been made.
• PAYE records - employee Pay History Records/national insurance records/staff and pension records.	7 years after employment ends.
• Payroll and wage records for companies	7 years after employment ends.
• Payroll and wage records for unincorporated businesses	7 years after employment ends.
• Records in relation to hours worked and payments made to workers	7 years after the employment ends.
• Travel and subsistence	7 years after employment ends.
• Record of advances for season tickets and loans to employees	7 years after employment ends.
Personnel Records	
• Qualifications/references. • Consents for the processing of special categories of personal data. • Annual leave records. • Annual assessment reports. • Disciplinary procedures. • Grievance procedures. • Death benefit nomination and revocation forms. • Resignation, termination and retirement. • References. • P45/46. • Health records.	7 years after employment ends.

• Internal applications/promotions/transfers/variation of contract • Flexible working request • TUPE/Secondment letters • Fit note/return to work/OH referral/OH report/risk assessment/ Ill health retirement/settlement/ Letter/notification/report/ Medical Redeployment Paperwork. • Probation/Review/appraisal. • Performance management documentation • Notice of resignation/leaver letter/exit interview/employment tribunal/settlement agreement.	
Records in Connection with Working Time	
• Working time opt-out	3 years from the date on which they were entered into.
• Records to show compliance, including: • Time sheets for opted-out workers. • Health assessment records for night workers.	3 years after the relevant period.
Maternity Records	
• Maternity payments. • Notification of maternity/return to work documentation. • Dates of maternity leave. • Period without maternity payment. • Maternity certificates showing the expected week of confinement. • Paternity notification and return to work documentation.	7 years after employment ends.
Accident Records	
• These are created regarding any reportable accident, death or injury in connection with work.	For at least 4 years from the date the report was made.
Company Documents	
• Accounting records detailing company transactions, including supporting documents	3 years from creation date.

• Register of members	Entries for former members can be removed 10 years after the date they ceased to be members.

• Formal company documents:
  ○ Statutory books
  ○ Board minutes
  ○ Resolutions
  ○ Register of directors
	Indefinitely.

• Meeting minutes	10 years from date of meeting.
• Audit documentation – reports, reports used during a fraud investigation, terms of reference	6 years after the legal proceedings have been competed or after the Committee has disbanded.
• Audit correspondence, working papers, local auditing standards, annual reports, minutes of meetings with the Audit Committee.	3 years.
• Supplier/consultancy documents • Contracts	6 years from end of contract.
Insurance Documentation	
• Employer's Liability Policy	Indefinitely.
VAT Records	
• Standard-rated goods • Exempt supplies • VAT account	6 years.
Corporation Tax Records	

• Records of all:
  ○ Company assets (e.g. receipts, sales and purchases)
  ○ Company liabilities
  ○ Income and expenses
  ○ Tax deduction or tax credit vouchers
	7 years.

All finance related documentation including: • Purchase orders • Invoices • Bank reconciliation files/sheet • Bank statements • Cash books (including petty cash books)	7 years.

• Statements of Accounts outstanding, outstanding orders • Statements of Accounts rendered, statements of accounts-payable • Ledgers and creditors ledgers • Financial statements • Trial balance records • Records relating to debts and overpayments • Investment records	
Records relating to serious matters of: • Theft • Fraud • Misappropriation • Irrecoverable debts and overpayments • Write-offs • Recovery of debt • Wavering of debt	10 years after action / investigation is completed (Where external action has been taken) or 7 years (Where matters are resolved internally).
Legal Records	
• Legal opinions and advice (non-litigation)	6 years after the matter that the advice relates to ends
• Legal advice and other records relating to specific litigation or claim.	6 years from settlement or withdrawal of claim
• Previous versions of policies, including IT policy, privacy policy, retention policy etc.	6 years from being superseded
• Monitoring and investigation requests	6 years from closure of investigation
• Insurance claims	3 years after settlement
• Data Subject Rights Requests – all related information	12 months after closure of request. 3 years if referred to Information Commissioner.
• FOISA or EIR requests and records	3 years after closure of request. 6 years if referred to SICO.
Procurement Records	
• Unsuccessful tenders	1 year after date of last paper
• Successful tenders	6 years from award of contract
Initial proposal – including: • End user requirements	6 years on completion of contract

• Statements of interest • Agreed specification • Evaluation criteria • Invitation to tender	
• Contractual documents and any documentation relating to the amendment/operation/extensions to the contracts	6 years from end of contract
IT Records	
• General information about internally developed IT infrastructure, software and systems for internal use.	5 years from decommissioning of system
• General information about externally developed IT infrastructure, software and systems for internal or external use.	7 years from decommissioning of system
• General information about internally developed IT infrastructure, software and systems for external use.	7 years from decommissioning of system
• Systems monitoring, (for example, to detect and prevent failures vulnerabilities and external threats).	• Current year plus 1 year • Consider whether records can be fully anonymised after this period (or no personal data collected in first place) where there is a need to keep these logs for longer or indefinitely
• Business continuity and information security plans.	• 3 years from when the plan is superseded • Consider whether record can be fully anonymised after this period (or no personal data collected in first place) where there is a contractual or legal obligation to keep these plans for a longer period.
• Technical support and help-desk requests.	• 3 years from end of system • Consider whether record can be fully anonymised after this period (or no personal data collected in first place) where there is a need to keep these requests for a longer period (for example, 7 years to align with limitation periods)

• Technical information relating to external customer user accounts.	• 1 year from account closure • Consider whether record can be fully anonymised after this period (or no personal data collected in first place) where there is a need to keep these plans for a longer period.
• Contracts and agreements (software licences, support agreements, hardware agreements etc.).	7 years from expiry of the agreement
• System backups.	3 months
• OneDrive	*24 months. (user to transfer any business information to appropriate SharePoint library).*
• SharePoint	2 years "last modified" default retention policy for documents. Ability for directorates to specify alternative retention periods.
Facilities and Security Records	
• CCTV recordings	• As long as necessary for any investigations or claims that arise
• Visitor logs	• 6 months
• Property management and asset records	6 years or 12 years depending on whether the agreement is executed as a simple contract or a deed respectively
• Building contracts	12 years from practical completion
• Leases	6 years from end of lease
• Health and safety files for building works	6 years from completion
Pensions Records	
• Name and address of scheme or provider of the automatic enrolment scheme used to comply with the employer's duties.	6 years
• Employer pension scheme reference.	6 years
• Evidence scheme complies with auto-enrolment statutory quality tests.	6 years

• Name, NI number, date of birth and automatic enrolment date of all jobholders auto-enrolled (and corresponding details for non-eligible jobholders and entitled workers who have opted in or joined).	6 years
• Evidence of jobholders' earnings and contributions.	6 years
• Contributions payable by employer in respect of jobholders and dates on which employer contributions were paid to scheme.	6 years
• If auto-enrolment postponement period used, records of workers who were given notice of postponement including full name, NI number and date postponement notice was given.	6 years
• Auto-enrolment opt-in notices, joining notices and opt-out notices (original format).	6 years (4 years for opt-out notices)
• If employer is (or was) sponsoring employer of an occupational pension scheme, any document relating to monies received by or owing to the scheme, investments or assets held by the scheme, payments made by the scheme, contracts to purchase a lifetime annuity in respect of scheme member and documents relating to the administration of the scheme.	For the tax year to which they relate and the following 6 years
• Information relating to applications for ill health early retirement benefits, including medical reports.	While entitlement continues and for period of 15 years after benefits stop being paid.
• Death benefit nomination and revocation forms.	While entitlement continues and for period of 15 years after the death of member and their beneficiaries.