Scottish Rail Holdings Limited

Data Protection Policy

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

Document Control

Title:	SRH Data Protection Policy
Reference:	SRH/Information & Data/6.2
Version:	1.0
Release Date:	19/05/2025
Author:	Neil Amner, General Counsel
Total Pages:	19 including preliminaries
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 draft 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 Data Protection Policy

1 Aim of this policy

1.1 This Data Protection Policy sets out how Scottish Rail Holdings Limited ("**we**", "**our**", "**us**", "**SRH**") handle the Personal Data of members of the public, suppliers, SRH Personnel, website users, business contacts or any other Data Subject.

1.2 We recognise that the correct and lawful treatment of Personal Data will maintain trust and confidence in the organisation and will provide for successful business operations. Protecting the confidentiality and integrity of Personal Data is a critical responsibility that we take seriously at all times. SRH is exposed to potential fines of up to £17.5 million or 4% of total worldwide annual turnover, whichever is higher and depending on the breach, for failure to comply with the UK GDPR.

1.3 Data protection is the responsibility of everyone within SRH and this Data Protection Policy sets out what we expect from SRH Personnel ("**you**", "**your**") when handling Personal Data to enable SRH to comply with applicable law.

2 Scope

2.1 This Data Protection Policy applies to all Personal Data we Process regardless of the media on which that data is stored or whether it relates to past or present members of the pubic, supplier contacts, SRH Personnel, website users, business contacts, or any other Data Subject.

2.2 This Data Protection Policy (together with Related Policies) is an internal document and cannot be shared with third parties, Scottish Ministers or regulators without prior authorisation from the GC.

2.3 Please contact the GC, failing which the DPO, with any questions about the operation of this Data Protection Policy or the UK GDPR or if you have any concerns that this Data Protection Policy is not being or has not been followed.

2.4 In particular, you must always contact the GC, failing which DPO, in the following circumstances:

- if you are unsure of the lawful basis on which you are relying to process Personal Data (including the legitimate interests used by SRH)
- if you need to rely on Consent or need to capture Explicit Consent
- if you need to draft Privacy Notices
- if you are unsure about the retention period for the Personal Data being Processed

- if you are unsure what security or other measures you need to implement to protect Personal Data
- if there has been a Personal Data Breach
- if you are unsure on what basis to transfer Personal Data outside the UK
- if you need any assistance dealing with any rights invoked by a Data Subject
- whenever you are engaging in a significant new, or change in, Processing activity which is likely to require a DPIA, or plan to use Personal Data for purposes other than for which it was collected
- if you plan to undertake any activities involving Automated Processing including profiling or Automated Decision-Making
- if you need help complying with applicable law when carrying out direct marketing activities
- if you need help with any contracts or other areas in relation to sharing Personal Data with third parties (including our suppliers)

3 Definitions

In this policy, the following words and phrases have the following meanings:

Automated Decision-Making (ADM): when a decision is made which is based solely on Automated Processing (including profiling) which produces legal effects or significantly affects an individual. The UK GDPR prohibits Automated Decision-Making (unless certain conditions are met) but not Automated Processing.

Automated Processing: any form of automated processing of Personal Data consisting of the use of Personal Data to evaluate certain personal aspects relating to an individual, in particular to analyse or predict aspects concerning that individual's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements. Profiling is an example of Automated Processing, as are many uses of artificial intelligence (AI) where they involve the processing of Personal Data.

Consent: agreement which must be freely given, specific, informed and be an unambiguous indication of the Data Subject's wishes by which they, by a statement or by a clear positive action, signify agreement to the Processing of Personal Data relating to them.

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 Privacy Impact Assessment (DPIA): tools and assessments used to identify and reduce risks of a data processing activity. A DPIA can be carried out as part of Privacy by Design and should be conducted for all major system or business change programmes involving the Processing of 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).

Explicit Consent: consent which requires a very clear and specific statement (that is, not just action).

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.

Personal Data Breach: any act or omission that compromises the security, confidentiality, integrity or availability of Personal Data or the physical, technical, administrative or organisational safeguards that we or our third-party service providers put in place to protect it. The loss, or unauthorised access, disclosure or acquisition, of Personal Data is a Personal Data Breach.

Privacy by Design: implementing appropriate technical and organisational measures in an effective manner to ensure compliance with the UK GDPR.

Privacy Notices (also referred to as Fair Processing Notices) or Privacy Policies: separate notices setting out information that may be provided to Data Subjects when SRH collects information about them. These notices may take the form of:

(a) general privacy statements applicable to a specific group of individuals (for example, employee privacy notices or the website privacy policy); or

(b) stand-alone, one-time privacy statements covering Processing related to a specific purpose.

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 Data Protection 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 We adhere to the principles relating to Processing of Personal Data set out in the UK GDPR which require Personal Data to be:

- Processed lawfully, fairly and in a transparent manner (**lawfulness, fairness and transparency**);
- collected only for specified, explicit and legitimate purposes (**purpose limitation**);
- adequate, relevant and limited to what is necessary in relation to the purposes for which it is Processed (**data minimisation**);
- accurate and where necessary kept up to date (**accuracy**);
- not kept in a form which permits identification of Data Subjects for longer than is necessary for the purposes for which the data is Processed (**storage limitation**);
- Processed in a manner that ensures its security using appropriate technical and organisational measures to protect against unauthorised or unlawful Processing and against accidental loss, destruction or damage (**security, integrity and confidentiality**);
- not transferred to another country without appropriate safeguards in place (**transfer limitation**); and

- made available to Data Subjects and allow Data Subjects to exercise certain rights in relation to their Personal Data (**data subject's rights and requests**).

6.2 We are responsible for and must be able to demonstrate compliance with the data protection principles listed above (**accountability**).

7 Lawfulness, fairness and transparency

7.1 Personal data must be Processed lawfully, fairly and in a transparent manner in relation to the Data Subject.

7.2 You may only collect, Process and share Personal Data fairly and lawfully and for specified purposes. The UK GDPR restricts our actions regarding Personal Data to specified lawful purposes. These restrictions are not intended to prevent Processing but ensure that we Process Personal Data fairly and without adversely affecting the Data Subject.

7.3 The UK GDPR allows Processing for specific purposes, some of which are set out below:

- the Data Subject has given their Consent;
- the Processing is necessary for the performance of a contract with the Data Subject or to take steps at the request of the Data Subject prior to entering into a contract;
- to meet our legal compliance obligations;
- to protect the Data Subject's vital interests;
- where it is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in us;
- to pursue our legitimate interests (or those of a third party) for purposes where they are not overridden because the Processing prejudices the interests or fundamental rights and freedoms of Data Subjects. The purposes for which we process Personal Data for legitimate interests need to be set out in applicable Privacy Notices.

7.4 You must identify and document the legal ground being relied on for each Processing activity.

8 Consent

8.1 A Controller must only process Personal Data on one or more of the lawful bases set out in the UK GDPR, which include Consent.

8.2 A Data Subject consents to Processing of their Personal Data if they clearly indicate agreement to the Processing. Consent requires affirmative action, so silence, pre-ticked boxes or inactivity will not be sufficient to indicate consent. If Consent is given in a document which deals with other matters, then the Consent must be kept separate from those other matters.

8.3 A Data Subject must be easily able to withdraw Consent to Processing at any time and withdrawal must be promptly honoured. Consent may need to be refreshed if you intend to Process Personal Data for a different and incompatible purpose which was not disclosed when the Data Subject first consented.

8.4 When processing Special Category Data or Criminal Convictions Data, we will usually rely on a legal basis for processing other than Explicit Consent or Consent if possible. Where Explicit Consent is relied on, you must issue a Privacy Notice to the Data Subject and ensure Explicit Consent is documented in writing.

8.5 You will need to evidence Consent captured and keep records of all Consents in accordance with Related Policies, so that SRH can demonstrate compliance with Consent requirements.

9 Notifying Data Subjects

9.1 The UK GDPR requires a Controller to provide detailed, specific information to a Data Subject depending on whether the information was collected directly from the Data Subject or from elsewhere. The information must be provided through an appropriate Privacy Notice which must be concise, transparent, intelligible, easily accessible, and in clear and plain language so that a Data Subject can easily understand them.

9.2 Whenever we collect Personal Data directly from a Data Subject, including for HR or employment purposes, we must provide the Data Subject with all the information required by the UK GDPR including the identity of the Controller and DPO, and how and why we will use, Process, disclose, protect and retain that Personal Data through a Privacy Notice which must be presented when the Data Subject first provides the Personal Data.

9.3 When Personal Data is collected indirectly (for example, from a third party or publicly available source), we must provide the Data Subject with all the information required by the UK GDPR as soon as possible after collecting or receiving the data but within one (1) month of receipt at the latest or if the Personal Data will be used to contact the data subject or a third party about the Data Subject, at the point of such communication. We must also check that the Personal Data was collected by the third party in accordance with the UK GDPR and on a basis which contemplates our proposed Processing of that Personal Data.

9.4 If you are collecting Personal Data from a Data Subject, directly or indirectly, then you must provide the Data Subject with a Privacy Notice in accordance with our Related Policies.

10 Purpose limitation

10.1 Personal Data must be collected only for specified, explicit and legitimate purposes. It must not be further Processed in any manner incompatible with those purposes.

10.2 You cannot use Personal Data for new, different or incompatible purposes from that

disclosed when it was first obtained unless you have informed the Data Subject of the new purposes and they have Consented where necessary.

10.3 If you want to use Personal Data for a new or different purpose from that for which it was obtained, you must first contact the GC, failing which the DPO for advice on how to do this in compliance with both the law and this Data Protection Policy.

11 Data minimisation

11.1 Personal Data must be adequate, relevant and limited to what is necessary in relation to the purposes for which it is Processed.

11.2 You may only Process Personal Data when performing your job duties requires it. You cannot Process Personal Data for any reason unrelated to your job duties.

11.3 You may only collect Personal Data that you require for your job duties: do not collect excessive data. Ensure any Personal Data collected is adequate and relevant for the intended purposes.

11.4 You must ensure that when Personal Data is no longer needed for specified purposes, it is deleted or anonymised in accordance with SRH's Data Retention Policy.

12 Accuracy

12.1 Personal Data must be accurate and, where necessary, kept up to date. It must be corrected or deleted without delay when inaccurate.

12.2 You must ensure that the Personal Data we use and hold is accurate, complete, kept up to date and relevant to the purpose for which we collected it. You must check the accuracy of any Personal Data at the point of collection and at regular intervals afterwards. You must take all reasonable steps to destroy or amend inaccurate or out-of-date Personal Data.

13 Storage limitation

13.1 Personal Data must not be kept in an identifiable form for longer than is necessary for the purposes for which the data is processed.

13.2 SRH will maintain retention policies and procedures to ensure Personal Data is deleted after an appropriate time, unless a law requires that data to be kept for a minimum time. You must comply with SRH's Data Retention Policy.

13.3 You must not keep Personal Data in a form which permits the identification of the Data Subject for longer than needed for the legitimate business purpose or purposes for which we originally collected it including for the purpose of satisfying any legal, accounting or reporting requirements.

13.4 You will take all reasonable steps to destroy or erase from our systems all Personal Data that we no longer require in accordance with all SRH's Data Retention Policy. This

includes requiring third parties to delete that data where applicable.

13.5 You will ensure Data Subjects are provided with information about the period for which data is stored and how that period is determined in any applicable Privacy Notice.

14 Security, integrity and confidentiality

14.1 Personal Data must be secured by appropriate technical and organisational measures against unauthorised or unlawful Processing, and against accidental loss, destruction or damage.

14.2 We will develop, implement and maintain safeguards appropriate to our size, scope and business, our available resources, the amount of Personal Data that we own or maintain on behalf of others, and identified risks (including use of encryption and Pseudonymisation where applicable). We will regularly evaluate and test the effectiveness of those safeguards to ensure security of our Processing of Personal Data. You are responsible for protecting the Personal Data we hold. You must implement reasonable and appropriate security measures against unlawful or unauthorised Processing of Personal Data and against the accidental loss of, or damage to, Personal Data. You must exercise particular care in protecting Special Categories of Personal Data and Criminal Convictions Data from loss and unauthorised access, use or disclosure.

14.3 You must follow all procedures and technologies we put in place to maintain the security of all Personal Data from the point of collection to the point of destruction. You may only transfer Personal Data to third-party service providers approved by SRH and who agree to comply with the required policies and procedures and who agree to put adequate measures in place, as requested.

14.4 You must maintain data security by protecting the confidentiality, integrity and availability of the Personal Data, defined as follows:

- **Confidentiality:** only people who have a need to know and are authorised to use the Personal Data can access it;
- **Integrity:** Personal Data is accurate and suitable for the purpose for which it is processed; and
- **Availability:** authorised users are able to access the Personal Data when they need it for authorised purposes.

14.5 You must comply with and not attempt to circumvent the administrative, physical and technical safeguards we implement and maintain in accordance with the UK GDPR and relevant standards to protect Personal Data.

15 Reporting a Personal Data Breach

15.1 In certain instances, the UK GDPR requires Controllers to notify a Personal Data Breach to the Information Commissioner and the Data Subject.

15.2 We have put in place procedures to deal with any suspected Personal Data Breach and will notify the Data Subject or any applicable regulator where we are legally required to do so or otherwise consider it appropriate to do so.

15.3 If you know or suspect that a Personal Data Breach has occurred, do not attempt to investigate the matter yourself. Immediately contact the General Counsel as the person designated as the key point of contact for Personal Data Breaches and follow SRH's Personal Data Breach Procedure. You should preserve all evidence relating to the potential Personal Data Breach.

16 Transfer limitation

16.1 The UK GDPR restricts data transfers to countries outside the UK to ensure that the level of data protection afforded to individuals by the UK GDPR is not undermined. You transfer Personal Data originating in one country across borders when you transmit, send, view or access that data in or to a different country.

16.2 You must comply with SRH's guidelines on cross-border data transfers.

16.3 You may only transfer Personal Data outside the UK if one of the following conditions applies:

16.3.1 the UK has issued regulations confirming that the country to which we transfer the Personal Data ensures an adequate level of protection for the Data Subject's rights and freedoms;

16.3.2 appropriate safeguards are in place such as binding corporate rules, standard contractual clauses approved for use in the UK, an approved code of conduct or a certification mechanism, a copy of which can be obtained from the GC, failing which the DPO (if such safeguards are available);

16.3.3 the Data Subject has provided Explicit Consent to the proposed transfer after being informed of any potential risks; or

16.3.4 the transfer is necessary for one of the other reasons set out in the UK GDPR including:

16.3.4.1 the performance of a contract between us and the Data Subject;
16.3.4.2 reasons of public interest;
16.3.4.3 to establish, exercise or defend legal claims;
16.3.4.4 to protect the vital interests of the Data Subject where the Data Subject is physically or legally incapable of giving Consent; and
16.3.4.5 in some limited cases, for our legitimate interest.

17 Transfer limitation

17.1 A Data Subject has rights when it comes to how we handle their Personal Data. These include rights to:

17.1.1 withdraw Consent to Processing at any time;
17.1.2 receive certain information about the Controller's Processing activities;
17.1.3 request access to their Personal Data that we hold (including receiving a copy of their Personal Data);
17.1.4 prevent our use of their Personal Data for direct marketing purposes;
17.1.5 ask us to erase Personal Data if it is no longer necessary in relation to the purposes for which it was collected or processed or to rectify inaccurate data or to complete incomplete data;
17.1.6 restrict Processing in specific circumstances;
17.1.7 object to Processing which has been justified on the basis of our legitimate interests or in the public interest;
17.1.8 request a copy of an agreement under which Personal Data is transferred outside of the UK;
17.1.9 object to decisions based solely on Automated Processing, including profiling (ADM);
17.1.10 prevent Processing that is likely to cause damage or distress to the Data Subject or anyone else;
17.1.11 be notified of a Personal Data Breach which is likely to result in high risk to their rights and freedoms;
17.1.12 make a complaint to the supervisory authority; and
17.1.13 in limited circumstances, receive or ask for their Personal Data to be transferred to a third party in a structured, commonly used and machine-readable format.

18 Accountability

18.1 The Controller must implement appropriate technical and organisational measures in an effective manner to ensure compliance with data protection principles. The Controller is responsible for, and must be able to demonstrate, compliance with the data protection principles.

18.2 SRH must have adequate resources and controls in place to ensure and to document UK GDPR compliance including:

18.2.1 appointing a suitably qualified DPO (where necessary) and an executive accountable for data protection;
18.2.2 implementing Privacy by Design when Processing Personal Data and completing DPIAs where Processing presents a high risk to rights and freedoms of Data Subjects;
18.2.3 integrating data protection into internal documents including this Data Protection Policy, Related Policies, or Privacy Notices;
18.2.4 regularly training SRH Personnel on the UK GDPR, this Data Protection Policy, Related Policies and data protection matters including, for example, a Data

Subject's rights, Consent, legal basis, DPIA and Personal Data Breaches. SRH must maintain a record of training attendance by SRH Personnel; and

18.2.5 regularly testing the data protection measures implemented and conducting periodic reviews and audits to assess compliance, including using results of testing to demonstrate compliance improvement effort.

19 Record Keeping

19.1 The UK GDPR requires us to keep full and accurate records of all our data Processing activities.

19.2 You must keep and maintain accurate corporate records reflecting our Processing including records of Data Subjects' Consents and procedures for obtaining Consents.

19.3 These records should include, at a minimum:

19.3.1 the name and contact details of the Controller and the DPO; and

19.3.2 clear descriptions of:

- the Personal Data types;
- the Data Subject types;
- the Processing activities;
- the Processing purposes;
- the third-party recipients of the Personal Data;
- the Personal Data storage locations;
- the Personal Data transfers;
- the Personal Data's retention period; and
- the security measures in place.

19.4 To create the records, data maps should be created which should include the detail set out above together with appropriate data flows.

20 Training and audit

20.1 We are required to ensure all SRH Personnel have undergone adequate training to enable them to comply with data privacy laws. We must also regularly test our systems and processes to assess compliance.

20.2 You must undergo all mandatory data privacy-related training and ensure your team undergoes similar mandatory training.

20.3 You must regularly review all the systems and processes under your control to ensure they comply with this Data Protection Policy and check that adequate governance controls and resources are in place to ensure proper use and protection of Personal Data.

21 Privacy by Design and Data Protection Impact Assessment (DPIA)

21.1 We are required to implement Privacy by Design measures when Processing Personal Data by implementing appropriate technical and organisational measures (like

Pseudonymisation) in an effective manner, to ensure compliance with data privacy principles.

21.2 You must assess what Privacy by Design measures can be implemented on all programmes, systems or processes that Process Personal Data by taking into account the following:

- The state of the art.
- The cost of implementation.
- The nature, scope, context and purposes of Processing.
- The risks of varying likelihood and severity for rights and freedoms of the Data Subject posed by the Processing.

21.3 The Controller must also conduct a DPIA in respect to high-risk Processing.

21.4 You should conduct a DPIA (and discuss your findings with the DPO) when implementing major system or business change programs involving the Processing of Personal Data including:

- Use of new technologies (programs, systems or processes, including the use of AI), or changing technologies (programs, systems or processes).
- Automated Processing including profiling and ADM.
- Direct marketing
- Large-scale Processing of Special Categories of Personal Data or Criminal Convictions Data.
- Large-scale, systematic monitoring of a publicly accessible area.

21.5 A DPIA must include:

- A description of the Processing, its purposes and the Controller's legitimate interests if appropriate.
- An assessment of the necessity and proportionality of the Processing in relation to its purpose.
- An assessment of the risk to individuals.
- The risk mitigation measures in place and demonstration of compliance.

21.6 You must comply with SRH's DPIA Procedure and Privacy by Design.

22 Sharing Personal Data

22.1 Generally, we are not allowed to share Personal Data with third parties unless certain safeguards and contractual arrangements have been put in place.

22.2 You must comply with SRH's Sharing Data with Third Parties Policy.

22.3 You may only share the Personal Data we hold with another employee, agent or representative of our group (which includes our subsidiaries) if the recipient has a job-

related need to know the information and the transfer complies with any applicable cross-border transfer restrictions.

22.4 You may only share the Personal Data we hold with third parties, such as our service providers, if:

22.4.1 they have a need to know the information for the purposes of providing the contracted services;

22.4.2 sharing the Personal Data complies with the Privacy Notice provided to the Data Subject and, if required, the Data Subject's Consent has been obtained;

22.4.3 the third party has agreed to comply with the required data security standards, policies and procedures, and put adequate security measures in place;

22.4.4 the transfer complies with any applicable cross-border transfer restrictions; and

22.4.5 a fully executed written contract that contains UK GDPR-approved third party clauses has been obtained.

23 Compliance

23.1 You must read, understand and comply with this Data Protection Policy when Processing Personal Data on our behalf and attend training on its requirements.

23.2 Your compliance with this Data Protection Policy is mandatory.

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

23.4 Any breach of this Data Protection Policy may result in disciplinary action.

23.5 Where you have a specific responsibility in connection with Processing, such as capturing Consent, reporting a Personal Data Breach or conducting a DPIA as referenced in this Data Protection Policy or otherwise, then you must comply with the Related Policies.

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

23.7 Where a breach of this policy or any of the Related Policies 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

24 Responsibilities

24.1 **SRH Board** are responsible for approval and formal support of this Data Protection Policy and Related Policies (together "**the Policies**").

24.2 **SRH General Counsel** has overall responsibility for and ownership of the Policies and 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.

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

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

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

- Their 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

25 Review and amendment

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

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

26 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:

- Appropriate Policy Document;
- Sharing of Personal Data with Third Parties Procedure;
- Personal Data Retention Policy;
- Employee Privacy Notice;
- Applicant Privacy Notice;
- DPIA Guidance;
- 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.