# Privacy Notice

**About us**
SAS and AIS are trading names of Sovereign Risk Management Limited (SRM), a UK company which is on the public register of data controllers, maintained by the Information Commissioner's Office. We arrange and administer both insurance and non-insurance services, such as fund management and wellbeing services for School Groups and Educational Associations throughout the UK.

We are responsible for marketing, administration, claims handling and provision associated with the services we offer. Our ICO license number is Z8122086.

Schools Advisory Service (SAS), Absence Insurance Services (AIS) are committed to ensuring your personal data is protected. This Privacy Notice provides details of the information that we may collect from you to assist with the administration and management of our relationship with you and the services we provide.

This notice sets out who we are, why we collect personal data, how we use that personal data, who we share the data with and how you can request access to that data or exercise other data subjects' rights.

Separate and specific Privacy Notices are provided to individuals when they:

- Access Medical and Wellbeing Service.
- When SRM requires access to individuals' medical records to support an insurance claim from the client.

This notice applies to:

- Clients which have entered into a contract for services or insurance policies with us or have begun the process of entering into a contract with us.
- The staff, and where appropriate insured person(s) and other stakeholders including governors and/or trustees, pupils and other authorised stakeholders of our clients.

This notice applies to data collected:

- Via our website
- Over the phone
- Via Email or other written communication
- Through our Wellbeing App
- And any other appropriate medium

**Data Protection Principles**
Personal Data must be processed in accordance with the six Data Protection Principles.
It must be:

- Used lawfully, fairly and in a transparent way.
- Collected only for valid purposes that we have clearly explained to you and not used in any way that is incompatible with those purposes.
- Relevant to the purposes we have told you about and limited only to those purposes.
- Accurate and kept up to date.
- Kept only as long as necessary for the purposes we have told you about.
- Kept securely.

This Privacy Notice sets out how SRM complies with these data processing principles.

**Where we might collect personal data from**
Depending on the information required we may collect personal data from various sources, including:

- The potential/actual client
- You (the data subject) as one of our client's stakeholders
- A Doctor, GP or other medical professionals in the event of a claim
- Anti-fraud databases, sanction list and other databases

We may, from time to time, receive information about you from the third parties we work with. This, for example, could be from a business partner or sub-contractor.

**Categories of personal data we collect**
We collect different categories of personal data depending on your relationship with us:

*Potential Clients*
If you have not entered into a contract for services or insurance policies with us but are considering doing so, we may collect:

- Details of the decision-makers within the organisation including name, position, email address and telephone number.
- Marketing preferences and customer satisfaction surveys.
- Phone calls which may be recorded for training or monitoring purposes.

*Clients*
If you have entered into a contract for services or insurance policies with us, or are in the process of renewing a contract with us, we may collect:

- Contact details of staff responsible for decision making for client(s), including name, position email address and phone number.
- Details of the staff member(s) authorised to administer the service/policy account including name, position and contact details and log-in details where applicable.
- Details of the client's staff, trustees and/or governors, pupils, and other authorised stakeholders nominated for one or more purposes in relation to the service contract or insurance policies including: name, date of birth, gender, position and job description,

working hours, details of pre-existing medical/health conditions and where relevant driving licence and driving convictions.
- Claim details which may include special category data such as health/medical information, union membership details and previous absence records.
- Phone calls which may be recorded for training or monitoring purposes.
- Marketing preferences and client satisfaction surveys.

*Wellbeing services*
The client provides SRM with limited personal data to enable their staff and other stakeholders to access medical and wellbeing services by contacting SRM directly. SRM is acting as the client's third-party processor in respect of this data. The client must meet their data protection obligations with regard to disclosure of third-party data processing and also document their lawful basis for providing this data to us in their Privacy Notices.

SRM also collects personal data directly from the staff member or other stakeholders when medical/wellbeing services are requested. In this respect, SRM is acting as a Data Controller.
The data may include: name, phone number, email address, postcode, date of birth, name of the client and postcode, a brief description of any concerns which may include health/medical data and customer feedback.

**How we use personal data**
We use personal data to:
- Provide quotations on request
- Manage your contract for services or insurance policy which may include administration, underwriting decisions and the processing of any related claims
- Send marketing or promotional information relating to SRM and its subsidiary groups
- Analyse the performance of our products and services
- Deliver medical and wellbeing services
- Comply with our legal and regulatory obligations
- Prevent and detect financial crime and fraud
- Assess financial and insurance risk

**Our Lawful Bases for Processing**
Whenever personal data is processed, SRM acting as a Data Controller must have a lawful basis for processing that data.
SRM processes general category personal data under the following lawful bases:

- Pursuant to a contract for services or an insurance policy, or to take steps to enter into a contract for services or an insurance policy
- To comply with a legal obligation
- For the legitimate interests of SRM or a third party (provided the individual's rights and freedoms are not overridden)
- The data subject has freely given clear consent

SRM processes special category personal data under the following lawful bases:
- The data subject has given their explicit consent

- To establish, exercise or defend legal claims

**Criminal Convictions**
SRM may process information relating to criminal convictions where the law allows us to do so.
It is envisaged SRM will hold information about criminal convictions in relation to driving convictions if this information comes to light as part of our due diligence checks in relation to an organisation's Minibus Insurance Policy, or if information about driving convictions comes to light during the term of a policy.

**Data Storage and Retention**
All data is kept on encrypted servers or encrypted back-up servers in the UK.

SRM will only keep personal information for as long as reasonably necessary to fulfil the relevant purposes for which the data was originally obtained. This will generally be for as long as:

- the contract of service or insurance policy is in force;
- in order to comply with legal and regulatory obligations, and
- as governed by the Limitations Act (1980).

SRM typically keep personal data for up to 7 years from the end of our relationship with you. In some cases, such as if there is a dispute or legal action, we may be required to keep personal information for longer.

**Who do we share personal data with?**
Insurance Services
In order to arrange and carry out your contract for services or an insurance policy, we may need to share personal data with third-party Data Controllers and Processors.
These may include:

- The Financial Conduct Authority;
- the Financial Ombudsman Service;
- any other regulator where so required; and
- our Policy underwriter, their agents and appointed representatives.

Wellbeing Services
Personal data may also be shared with third-party service providers or appointed representatives who deliver specific Medical and Wellbeing services or activities.

In all instances SRM will:

- Establish a data-sharing agreement with the supplier or contractor, either in the contract or as a standalone agreement, to ensure the fair and lawful processing of any personal data in accordance with our policies and Data Protection legislation; and
- only share data that the supplier or contractor needs in order to deliver their service, and information necessary to keep them safe while working with us.

Others
We may also share the contact details of our Clients with service providers whom we believe will be of interest to you.

Your personal data may also be shared in the event of a merger, asset sale or other related transaction such as a change in policy underwriter.

**Data Security**

SRM have put in place appropriate security measures to prevent your personal information from being accidentally lost, used or accessed in an unauthorised way, altered or disclosed. In addition, access to your personal information is limited to those employees, consultants, contractors and other third parties who have a business need to know. They will only process your personal information on our instructions, and they are subject to a duty of confidentiality.

We have in place procedures to deal with any suspected data security breach and will notify you and any applicable regulator of a suspected breach where we are legally required to do so and in accordance with our Data Security Policy and Breach Procedure.

**Your Data Subject Rights**

Individuals have the right to:

- Make a Subject Access Request (SAR) (see below);
- Withdraw consent to data processing at any time where consent is the sole lawful basis for the processing of that data;
- Ask us to rectify, erase or restrict processing of your personal data, or object to the processing of it (in certain circumstances);
- Prevent use of your personal data for direct marketing;
- Challenge processing which has been justified on the basis of legitimate interests;
- Request a copy of agreements under which your personal data is transferred outside of the European Economic Area, if relevant;
- Object to decisions based solely on automated decision making or profiling. SRM does not use automated decision making and/or profiling in any of its processes and procedures;
- Prevent processing that is likely to cause damage or distress;
- Be notified of a data breach in certain circumstances;
- Make a complaint to the ICO; and
- Ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format (in certain circumstances).

Subject Access Requests (SARs)

Under data protection legislation, individuals have the right to request access to their personal data held by SRM. Where SRM acts as a Data Controller Subject Access Requests may be made directly to SRM.

A helpful 'Guide to Making A Subject Access Request' is available from the SRM office, or as a download from our website https://schooladvice.co.uk/

It is not mandatory to make a Subject Access Request using the form. It will, however, assist in structuring the SAR to provide the information necessary to ensure we can action your request without delay.

Where a SAR or any other data subject rights' request is received in relation to the personal data provided to us by our client(s) (Data Controller), and where SRM is acting as the organisation's Data Processor, the SAR will be forwarded to the Data Controller, SRM's Client(s), without response.

SRM shall assist their Client(s) in the fulfilment of their obligation to respond to any Data Subject Request if the reply to a request requires our assistance and the provision of information and documentation.

Fulfilling A Subject Access Request

The lawful timescale for responding to a Subject Access Request is one calendar month from receipt of a 'valid' SAR.

A SAR is only considered 'valid' when we are fully satisfied regarding the identity of the requester and their entitlement to the data requested. If in any doubt we will request confirmation of identity to ensure your personal data is not inadvertently released to a third-party who is not entitled to it.

If the SAR is complex or numerous, the period in which we must respond may be extended by a further two months. You will be notified of any delays in actioning the SAR and provided with a time frame within which you can expect to receive the requested data.

Fees

You will not have to pay a fee to access your personal information (or to exercise any of your other data subject rights). However, we may charge a reasonable fee if your request for access is manifestly unfounded or excessive. Alternatively, we may refuse to comply with the request in such circumstances.

Exercising Other Data Subject Rights

If you wish to review, verify, correct or request the erasure of your personal information, object to the processing of your personal data, or request that we transfer a copy of your personal information to another party, please contact SRM in the first instance (details below).

The Right to Withdraw Consent

Where you may have provided your consent to the collection, processing and transfer of your personal information for a specific purpose – e.g. the provision of medical/wellbeing service, and there is no other lawful basis for processing the data, you have the right to withdraw your consent for that specific processing at any time.

To withdraw your consent, please contact SRM. Once we have received notification that you have withdrawn your consent, we will no longer process your information for the purpose or purposes you originally agreed to, unless we have another legitimate basis for doing so in law.
If we are prevented or restricted from processing personal information, we may not be able to provide the full benefits of the Agreement to you.

**Contacts**

**Data Controller**: Sovereign Risk Management, Trigg House, Maisies Way, South Normanton. DE55 2DS

If you have any questions or concerns about how we process personal data, or you wish to exercise any data protection rights, please email your query to dpo@uk-sas.co.uk

Or, write to:
**Data Protection Officer**, Trigg House, 11 Maisies Way, South Normanton, Derbyshire, DE55 2DS.

If you have concerns that we are not able to resolve to your satisfaction you can register a concern with the UK's data protection regulator, the Information Commissioner's Office by following this link https://ico.org.uk/make-a-complaint/

Or, write to:
Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire. SK9 5AF
Tel: 0303 123 1113

**Monitoring & Review**
This Privacy Notice will be reviewed on a yearly basis or as necessary in relation to changes in Data Protection legislation.

We reserve the right to update this Privacy Notice at any time, and we will provide you with a new Privacy Notice when we make any substantial updates.

| | |
|---|---|
| Effective Date: | May 2018 |
| Last update: | April 2020 |
| Review Date: | April 2021 |