Scottish Geology Trust Data Processing Policy

Version 1.0 Approved by Board of Trustees on 2023-01-24.

Policy Scope and Introduction

This policy describes the Scottish Geology Trust's (SGT) commitment to protecting personal data and complying with UK data processing and protection laws and regulations , including the Data Protection Act 2018 (the UK's implementation of the General Data Protection Regulation – GDPR),and the Privacy and Electronic Communications Regulations (PECR).

This policy applies to all personal data that is processed by SGT and it's representatives, irrespective of who created the data, the format of the data, or where the data is held. This includes publicly available data.

As part of its charitable activities, SGT will process personal data belonging to:

- Trustees, volunteers, and staff (contracted or employed) who represent SGT.
- Individuals within organisations that the trust interacts with, such as project partners, universities, societies, media outlets, and community associations.
- Members, donors, supporters, and members of our mailing list.
- Event participants.
- Members of the public who contact us through various channels, including email and social media.
- People we have reason to believe would be interested in the work of SGT.
- Other stakeholders for Scotland's geological heritage.

SGT does not expect to process personal data of children or vulnerable adults. If such data processing becomes likely, additional risk assessments need to be carried out and this policy revised accordingly.

When SGT or its representatives processes personal data for SGT's purposes, SGT is the data controller and is responsible for complying with data protection laws. It is therefore important that all of SGT's representatives understand and comply with this policy, to ensure that SGT can meet its legal obligations.

SGT aspires to incorporate the principle of "data protection by design" into all its activities, whilst balancing the operational needs of a small, resource-poor charity.

The data protection principles

Data protection laws are based on 7 data protection principles. This section briefly summarises each principle and describes how SGT complies with that principle. More information can be found in SGT's Data Processing Handbook, or the ICO Website.

1. Lawfulness, Fairness, and Transparency

We must have a valid reason (lawful basis) to process data, we must use it in a way that is fair and does not interfere with the rights of the individual, and we must be open and honest about how we use the data.

The lawful bases for processing personal data are: consent, contract, legal obligation, vital interests, public task, and / or legitimate interest. We may have more than one lawful basis for processing data. More information on the lawful bases is available in SGT's Data Processing Handbook, or on the ICO Website.

To comply with this principle, SGT maintains a Data Processing Register (DPR) for all data processing activities. The register identifies the lawful basis or bases for data processing and establishes the fairness of the data processing activity via an appropriately detailed risk assessment. SGT issues privacy notices as appropriate.

2. Purpose Limitation

We must be clear about our purposes for processing personal data, and record this purpose. We can only use personal data for a new purpose if it is compatible with our original purpose, we have consent, or we have a clear legal obligation.

To comply with this principle, SGT records the purpose for processing personal data in its Data Processing Register. Any new use of data is to be treated as a new data processing activity, undergo the appropriate risk assessment, and generate and issue appropriate privacy notices.

3. Data Minimisation

We must ensure that the data we are processing is sufficient to fulfil our intended purpose, relevant, and limited to what is necessary to fulfil that purpose.

SGT complies with this principle by avoiding collection and holding of unnecessary personal data, and periodically reviewing our data processing activities and the data we hold.

4. Accuracy

While SGT does not process data in a way that a lack of accuracy would affect the right of the individual, we must take reasonable steps to ensure the personal data we hold is correct and up to date.

SGT complies with this principle by committing to correct any mistakes that are discovered or notified, and ensuring that matters of opinion are clearly recorded as opinions rather than facts.

5. Storage Limitation

We must not keep personal data for longer than we need it, and we must be able to justify how long we keep personal data.

SGT complies with this principle by incorporating data retention in our data processing assessments, and noting required retention periods in our Data Processing Register.

SGT aspires to create a Data Retention Policy that establishes standard data retention periods for different types of data, and procedures for reviewing and either deleting or anonymising data which is no longer needed.

6. Integrity and Confidentiality (Security)

We must ensure that we have appropriate security measures in place to protect the data that we hold.

SGT complies with this principle by carrying out a risk assessment for all data processing activities, recording the result in the Data Processing Register, and adopting appropriate security measures.

7. Accountability

We must take responsibility for what we do with personal data and have appropriate records in place to demonstrate compliance.

SGT complies with this principle by maintaining the data processing and carrying out more in depth risk assessments where appropriate, including legitimate interest assessments, data processing impact assessments, and data transfer risk assessments. We also maintain a Data Protection Breach Register, which will hold details of any data protection breaches, regardless of whether they are serious enough to be notified to ICO.

Rights of individuals

Individuals have rights concerning their personal data. This section describes those rights and how SGT complies with those rights.

The right to be informed

Individuals have the right to know what data SGT collects and holds about them, where we get the data from, and what we do with it. SGT complies with this right by issuing privacy notices that describe this information. If a form of data processing is not covered in the appropriate privacy policy, then a new data processing risk assessment needs to be completed and privacy notices

issued as soon as possible. It is feasible that there might be rare circumstances where it is in the best interests of all parties for SGT to process data without telling the individual. The possibility of such activities is identified in the global privacy notice, but such activities will nevertheless require a full data processing impact assessment.

The right of access

Individuals have the right to ask SGT whether we use or store their personal information, how so, and for copies of the information we hold about them. Such a request is a Subject Access Request (SAR). If SGT receives a SAR from an individual, we must respond within one calendar month and cannot charge a fee. All SARs should be discussed with SGT's Executive Committee as soon as possible.

The right to rectification

Individuals have the right to request that we correct data held about them. They can make this request verbally or in writing, and to any representative of the organisation. SGT has one calendar month to respond to the request. Any requests for rectification should be forwarded to SGT's Executive Committee as soon as possible.

The right to erasure

Individuals have "the right to be forgotten" in some circumstances. Requests can be made verbally or in writing, and SGT must respond within one month. The right to erasure only applies to data held at the time of request and does not apply to data created in the future. The right only applies if:

- the personal data is no longer necessary for the purpose that we originally collected it for; or
- we are relying on consent to process the data and the consent has been withdrawn; or
- we are relying on legitimate interest as the lawful basis of processing and there is no overriding legitimate interest to continue that processing; or
- we are processing their data for direct marketing and the individual objects to that processing;

The right to object

Individuals have an absolute right to stop their data being used for direct marketing. For SGT's purposes, this includes all communications sent to specific individuals that promote SGT's charitable aims. In some circumstances, individuals may have the right to object to other forms of data processing, too. Individuals may make their objection verbally or in writing and SGT has one calendar month to respond.

The objection may relate to all the data we hold about an individual, or just part of the data, or just specific uses of the data.

The right to object to processing is most applicable to data processing with a legitimate interest lawful basis. The individual must give their reasons for objecting. SGT can refuse to comply with the

request if we can demonstrate compelling legitimate grounds for continuing the processing that override the interests, rights, and freedoms of the individual, or if the processing is related to a legal claim.

The right to restrict processing

In some circumstances, individuals have the right to request that we restrict processing of their data. This would mean we are expected to continue storing their data, but not process or use it in any other way. This right has similarities to the right to erasure or the right to object. Requests can be made verbally or in writing, and SGT must respond within one month.

The most likely scenario that SGT will encounter regarding this right is if an individual has objected to data processing on legitimate interest grounds, and we are considering whether our interests override those of the individual. In such circumstances, an individual may request restriction of processing while we make a decision, and it is good practice to restrict data processing regardless of whether a request is made.

The right to data portability

Individuals have the right to obtain and reuse their personal data for their own purposes across different services. This right is not currently relevant for SGT's data processing activities but may be relevant if SGT creates online forums or facilitates citizen science type programs.

Rights in relation to automated decision making and profiling.

Individuals have the right to object to being the subject of automated decision making and profiling. These are not activities that SGT are involved with.

Service providers and data transfers

SGT may use third party service providers to achieve its charitable aims. These include payment services (e.g. WebCollect, GoCardless, Paypal), registration services (e.g. WebCollect, MailChimp), email providers (e.g. LCN, gmail, other personal email addresses), cloud storage services (e.g. Dropbox), and other services as appropriate.

Each of these cases involves transferring of personal data to a third party, and sometimes that third party, and / or the server they store data on, may be located in a different country that does not have a data protection adequacy agreement with the UK. In most cases, SGT will remain the controller of the personal data, and the third party will be a data processor, acting on SGT's instructions.

To comply with the Security principle, while balancing SGT's operational needs and lack of resources during our early growth phase, we will perform due diligence risk assessments when selecting a new service or reviewing contracts with existing services. These risk assessments will be recorded in the document "Data Processing Assessment for Third Parties" and, in particular, will

ensure that third parties do not have the right to access or use the data for their own purposes. These assessments may include a restricted data transfer assessment, if use of the third party involves transfer of data to a country without data protection adequacy agreements.

Personal Data Breaches

A personal data breach involves the unlawful destruction, loss, alteration, unauthorised disclosure, or unauthorised access to personal data. Data breaches may be accidental or deliberate. They are a security incident that affects the confidentiality, integrity, or availability of personal data.

Responses to data breaches need to mitigate any negative impact for the individual whose data has been breached, and consider operational changes to reduce the chance of such an incident happening again. Each breach should be considered on a case-by-case basis.

If the data breach poses a high risk to the individual(s), they should be informed as soon as possible. Data breaches need to be reported to ICO unless we can demonstrate that the breach is unlikely to result in a risk to the rights and freedoms of the affected individuals. Reports to ICO need to be made as soon as possible, and within 72 hours of becoming aware of the breach. Our decision making process regarding each data breach needs to be documented in the data breach register.

If you become aware of a personal data breach, or a near miss, you should inform SGT's Executive Committee as soon as possible, and work with them to assess the risk and appropriate action. SGT recognises that mistakes happen, and does not condone reprimanding individuals for isolated mistakes. Individuals working within SGT should promote a culture where people feel safe to report mistakes, as this will help us comply with our obligations to assess and report data breaches within the appropriate timeframe.

Data Protection Responsibilities within SGT

SGT's Executive Committee (EC) is the first point of contact for data processing queries. The EC is responsible for monitoring data processing activities and risk assessments, reviewing this data processing policy, reviewing and optimising data processing procedures, and ensuring our data processing registration with ICO is maintained and up to date. EC members, especially the Secretary, Chair, and Vice Chairs, are thus expected to familiarise themselves with the contents of the SGT Data Processing Handbook.

However, any individual representing SGT is responsible for ensuring their activities are compliant with this policy and the data protection law. In particular, SGT representatives are expected to:

- Read and understand this policy.
- Understand that publicly available personal data is still covered by data protection regulations.
- Recognise that special category personal data (racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic, biometric, or health data, sexual orientation, or data concerning a person's sex life) and data about children

require higher protections and that extra care needs to be taken if you process this data, even inadvertently.

- Recognise when a new activity involves processing of personal information and then:
    - Familiarise themselves with the contents of the SGT Data Protection Handbook
    - Carry out a data processing assessment (see next section)
    - Inform the EC of the assessment and outcome
    - Only proceed with the new data processing activity once the activity has been approved (see next section).
    - Work with the EC to draft a new privacy notice, if appropriate.
- Recognise that ICO considers all communications that draw attention to a charity's aims and campaigns to be marketing activities and are therefore subject to PECR. This means individuals can only be contacted electronically (email, social media) if they have explicitly given consent to receive unsolicited marketing from us. Emails that are designed to raise awareness of SGT, should thus only be sent to individuals via SGT email accounts or in your capacity as a SGT representative, **if** we have their consent (i.e. they signed up to the mailing list), or to respond to a query.
- Take steps to maintain good cyber-security measures.
- Practice good email etiquette:
    - Where possible, do not forward emails or documents without permission of the original author.
    - Use the "check twice, send once" principle, especially regarding recipient email addresses.
    - Delete emails that are no longer necessary, within 6 years of the email subject being resolved.
    - Do not "gossip" or discuss superfluous information about people, especially in email chains related to SGT business.
- Report any data protection breaches or near misses to the EC as soon as you become aware of them, and help the EC with the risk assessment process.
- Notify the EC as soon as possible if you receive a request from an individual exercising their data processing rights.
- Not store any files containing sensitive personal information on Dropbox.

Data Processing Assessment Procedures

This section gives an overview of SGT's data processing procedures. Detailed data processing risk assessment procedures are described in the Data Processing Register.

1. When a new data processing activity is identified, first consult the Data Processing Register to see whether the activity is covered under an existing assessment.
2. If not, notify the EC and complete a new entry in the Data Processing Register.
3. If a legitimate interest lawful basis is invoked, a legitimate interest assessment also needs to be carried out. Check the existing assessments to see whether your activity is covered under an existing assessment.

4. If the activity involves an international data transfer (which may include transfer of data to a third party service provider with servers outside of the UK), consider whether or not this is a restricted transfer (Third Parties Assessment may be required) and if so, complete the Restricted Transfer Assessment (RTA).
5. If an RTA requires it, or your initial assessment is a medium or high risk, complete a data processing impact assessment (DPIA).
6. Initial and date the entry in the Data Processing Register, and ask another trustee to review the assessment. If the person carrying out the assessment is not a trustee, 2 trustees should review the assessment.
7. If the review disagrees with the original assessment and a revised assessment cannot be agreed on, refer the assessment to SGT's Executive Committee.
8. If both trustees agree that the activity is low risk:
    a. the activity is approved from the date when the second trustee adds their initials and date.
    b. A privacy notice should be drafted in consultation with SGT's Executive Committee, and issued in an appropriate timescale and manner.
9. If both trustees agree that the activity is medium to high risk, but that the benefits of proceeding outweigh the risk, the decision must be referred to the board for approval.

The Data Processing Register and processing assessments are held in SGT's cloud storage in a folder named "Data Processing Assessment".

All trustees are expected to periodically review and familiarise themselves with the contents of Data Processing Register and consider whether it adequately covers SGT's data processing activities.

Privacy Notices

This data processing policy describes SGT's policy, responsibilities, and commitments regarding processing of personal data. In the interests of transparency, it should be made available on SGT's website. However, it is intended as an internal document to guide governance and practice. Instead of a privacy policy targeted at a public audience, we use privacy notices.

Privacy notices are similar to policies, but provide targeted information of most interest to the individual, or group of individuals, concerned. They are designed to fulfil our data protection principle obligations by explaining what data we collect, why we need it, what we will do with it, whether we will share it, how long we can keep it, and what rights individuals have regarding their data.

SGT Privacy notices include:

- A global privacy notice hosted on our website, and a link provided in all SGT emails sent outside the organisation.
- An SGT members, supporters, and volunteers privacy notice, provided at membership registration, and available on the website with a link provided in all membership communication emails.

- A mailing list membership privacy notice, provided at mailing list registration, and available on the website with a link provided in all mailing list emails.
- A privacy notice for SGT Trustees – provided when a trustee joins the trust and available on the website.
- A privacy notice for staff and contractors, provided during contractual negotiations and available on the website.
- A privacy notice for potential supporters, provided at first contact or within a month of processing the data, whichever is soonest.

Updates to this policy

This policy will need to be updated as SGT's data processing activities evolve and our membership and audience bases increase.

Policy review should be carried out:

- At least every 2 years.
- When SGT membership reaches 400, or our mailing list reaches 500.
- If we identify a change in our data processing activities that require a change in policy, for example a change to our cloud storage provider.
- If a data processing risk assessment identifies a need to update this policy.

Change Record

Date of Change:	Changed By:	Comments:	Version
24/Jan/2023	Board	Policy approved by the Board	1.0