

## Data Protection and Use Policy

### Introduction

The security and management of data is important to ensure that the Geographical Association (GA) can function effectively and successfully for the benefit of its members. In doing so, it is essential that people's privacy is protected through the lawful and appropriate use and handling of their personal information.

The use of all personal data by the GA is governed by:

- The General Data Protection Regulation (GDPR)
- The UK Data Protection Act 2018 (DPA)
- The Privacy and Electronic Communications Regulations (PECR).

The ultimate responsibility for data protection rests with the Governing Body and Chief Executive in lieu of nominating a Data Protection Officer. The GA's senior leadership team will be responsible for the enactment this policy. This policy will be reviewed on a periodic basis by the Governing Body.

### Definitions

**Data** is defined as all material used, stored or processed by the Geographical Association.

**Personal data** means data which relate to a living individual who can be identified

- from those data, or
- from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller, and includes any expression of opinion about the individual.

**Sensitive personal data** means personal data consisting of information as to:

- the racial or ethnic origin of the data subject
- their political opinions
- their religious beliefs or other beliefs of a similar nature
- whether they are a member of a trade union
- their physical or mental health or condition
- their sexual orientation
- the commission or alleged commission by them of any offence.

### Who does this policy apply to?

The GA's data protection policy applies to all GA employees and all volunteer groups – including special interest groups, phase committees, working groups and communication boards.

GA Branches should be made aware of the GA's data protection policy, although data protection activity and the management of their own data is the individual responsibility of each branch.

### **Data protection principles**

The GA complies with the data protection principles set out below. When processing personal data, it ensures that:

- it is processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency')
- it is collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes ('purpose limitation')
- it is all adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation')
- it is all accurate and, where necessary, kept up to date and that reasonable steps will be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy')
- it is kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed ('storage limitation')
- it is processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality').

The GA will facilitate any request from a data subject who wishes to exercise their rights under data protection law as appropriate, always communicating in a concise, transparent, intelligible and easily accessible form and without undue delay.

### **Data Subject Rights**

The GA has processes in place to ensure that it can facilitate any request made by an individual to exercise their rights under data protection law. All staff have received training and are aware of the rights of data subjects. Staff can identify such a request and know who to send it to.

All requests will be considered without undue delay and within one month of receipt as far as possible.

- Subject access: the right to request information about how personal data is being processed, including whether personal data is being processed and the right to be allowed access to that data and to be provided with a copy of that data along with the right to obtain the following information:
  - the purpose of the processing
  - the categories of personal data
  - the recipients to whom data have been disclosed or which will be disclosed
  - the retention period
  - the right to lodge a complaint with the Information Commissioner's Office

- the source of the information if not collected direct from the subject, and
- the existence of any automated decision making
- Rectification: the right to allow a data subject to rectify inaccurate personal data concerning them.
- Erasure: the right to have data erased and to have confirmation of erasure, but only where:
  - the data is no longer necessary in relation to the purpose for which it was collected, or
  - where consent is withdrawn, or
  - where there is no legal basis for the processing, or
  - there is a legal obligation to delete data
- Restriction of processing: the right to ask for certain processing to be restricted in the following circumstances:
  - if the accuracy of the personal data is being contested, or
  - if our processing is unlawful but the data subject does not want it erased, or
  - if the data subject has objected to the processing, pending verification of that objection
- Data portability: the right to receive a copy of personal data which has been provided by the data subject and which is processed by automated means in a format which will allow the individual to transfer the data to another data controller. This would only apply if the GA was processing the data using consent or on the basis of a contract.
- Object to processing: the right to object to the processing of personal data relying on the legitimate interests processing condition unless the GA can demonstrate compelling legitimate grounds for the processing which override the interests of the data subject.

### **Reporting of breaches**

A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data

All members of staff should be vigilant and able to identify a suspected personal data breach. A breach could include:

- loss or theft of devices or data
- hacking or other forms of unauthorised access to a device, email account, or the network
- disclosing personal data to the wrong person, through wrongly addressed emails, or bulk emails that inappropriately reveal all recipients email addresses
- alteration or destruction of personal data without permission.

Where a member of staff discovers or suspects a personal data breach, this should be reported to the Finance and Operations Manager as soon as possible.

Where there is a likely risk to individuals' rights and freedoms, the Finance and Operations will report the personal data breach to the Information Commission Office (ICO) within 72 hours of the

organisation being aware of the breach. Where there is also a likely high risk to individuals' rights and freedoms, The GA will inform those individuals without undue delay.

The Finance and Operations Manager will keep a record of all personal data breaches reported, and follow up with appropriate measures and improvements to reduce the risk of reoccurrence.

### **Employees**

The GA ensures that good data protection practice is imbedded in the culture of our staff and our organisation. GA staff will be provided with adequate training into the GDPR principles and are required to observe the procedures as outlined in the GA Employee Handbook. These procedures and rules will be reviewed by the SLT and reminders and further training to be provided as appropriate.

### **Other formal documents relevant to this policy**

- Privacy Notice
- Record of processing activities
- Disaster Recovery policy
- Equal Opportunities Policy
- Media Policy
- Staff Handbook

**Last updated 2021**