Data protection and use policy

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
(a) from those data, or
(b) 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:
(a) the racial or ethnic origin of the data subject,
(b) their political opinions,
(c) their religious beliefs or other beliefs of a similar nature,
(d) whether they are a member of a trade union
(e) their physical or mental health or condition,
(f) their sexual life,
(g) the commission or alleged commission by them of any offence.

Other policies
This policy is related to the following other GA policies and should be used in consideration of them: Disaster Recovery, Equal Opportunities and Media.

Classification
Some data may be classified by the Senior Management of the GA as confidential with restricted circulation. This data will be designated as confidential for commercial or business reasons and will be marked as such.

Legal requirements
The Geographical Association complies with the Data Protection Act 1998 (DPA).

The General Data Protection Regulations (GDPR) replaces the Data Protection Act and applies from May 2018. GDPR is designed to ‘harmonise’ data privacy laws across Europe as well as give greater protection and rights to individuals and how their personal information is handled, processed and stored. It requires organisations to re-evaluate how they conduct the processing of personal data and places a greater emphasis and expectation on how organisations can demonstrate sound accountability and governance of the personal data that they process.
Who does this apply to?
The GA's data protection policy applies to all GA employees, and all volunteer groups – the special interest groups, phase committees 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.

Compliance
The GA observes the eight data protection principles, as follows. Data shall be:

- fairly and lawfully processed
  Under the terms of the DPA and GDPR and will not be shared with other parties without their express permission - this will be checked by senior managers from time to time. Examples include: lists of course or conference delegates should not be shared with third parties
- processed for limited purposes
  Limited for specific use within the GA and by its Committees - checked by senior managers. Examples include: membership records
- adequate, relevant and not excessive
  Checks will be made by senior managers from time to time on the data collected to see that this is the case
- accurate
  Data will be updated on a regular basis to ensure that it remains accurate, Examples include: email addresses requested when renewing membership.
- not kept longer than necessary
  Data will only be kept for a specific period which is to be defined on a case-by-case basis according to context and GDPR requirements. Business data will be kept for the prescribed time. Data may be archived for research purposes only. Senior managers to check annually.
- processed in accordance with the data subjects’ rights*
  Verified by the senior manager from time to time
- secure;
  Stored in a secure place with limited access to members of the GA staff and members of the GB – See Disaster recovery policy
- not transferred to countries outside the United Kingdom without adequate protection.

* See Appendix

In addition, the GA:

- has made data processing and privacy statements available on the website.
- needs to be aware of an individual’s right to erasure (also known as ‘the right to be forgotten’). The broad principle underpinning this right is that an individual can request the deletion or removal of their personal data.
• should be aware of an individual’s right to ‘data portability’. In essence, this means an employee can request that their personnel details be exported in electronic format or transferred to another system.

• is aware that it has a duty to report certain types of data breach to the ICO, and in some cases to the individuals affected. A notifiable breach is one where there is significant risk/detrimental effect to the individual/s affected such as the risk of data theft or risk of financial loss.

• will ensure that in its marketing activities consent is freely given, specific, informed and unambiguous. There must be a positive opt-in – consent cannot be inferred from silence, pre-ticked boxes or inactivity. It must also be separate from other terms and conditions, and there should be simple ways for people to withdraw consent.

**Employees are required to observe the following rules** (clause 5.31 of the GA Employee Handbook):

The GA holds personal data on members, employees and others and must comply with current data protection legislation.

• Do not divulge personal information about any GA members or other contacts without their express permission

• Be particularly careful when responding to enquiries about member/customer personal accounts in case the enquirer is not who they say they are

• Do not leave personal data on screen or as paperwork on your desk where visitors might see it

• Staff responsible for GA mail-shots or web site (paper or e-mail or other electronic means) must ensure that they comply with the Data Protection and GDPR rules about direct marketing.

• Personal identification information should not be divulged to Committees or Branches except for names and general locations but not specific locations.

*Verification of these rules will be checked by a senior manager and reminders issued from time to time.*

The ultimate responsibility for data protection rests with the Named Trustees and Chief Executive.

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.

Appendix

Data subjects’ rights are defined as follows:

1. The right to be informed
2. The right of access
3. The right to rectification
4. The right to erasure
5. The right to restrict processing
6. The right to data portability
7. The right to object
8. Rights in relation to automated decision making and profiling.