

## **Data Protection Policy**

---

### **Regional Studies Association**

Updated November 2020

This document contains information about:

- Policy application
- Principles of data protection
- Handling personal/special category information
- The person responsible for implementation
- Notification to the Information Commissioner
- Privacy/Personal Information Management of
  - RSA employees
  - RSA Board members

The Regional Studies Association is a Company Limited by Guarantee  
Company Number 04116288, Registered Charity Number 1084165.

# Data Protection Policy

---

## 1. Introduction

The Regional Studies Association is fully committed to compliance with the requirements of the Data Protection Act 2018 (“the Act”) and the General Data Protection Regulations (“GDPR”) which came into force on 25 May 2018. The Association will therefore follow procedures to ensure that all employees, elected officials, contractors, agents, consultants, partners or members of the Association who have access to any personal data held by or on behalf of the Association are fully aware of and abide by their duties and responsibilities under the Act.

## 2. Statement of policy

In order to operate efficiently, the Regional Studies Association has to collect and use information about people with whom it works. These may include members of the Association, current, past and prospective employees, clients and customers, and suppliers. In addition, it may be required by law to collect and use information in order to comply with the requirements of central government. This personal information must be handled and dealt with properly, however it is collected, recorded and used, and whether it be on paper, in computer records or recorded by any other means, and there are safeguards within the Act to ensure this.

The Association regards the lawful and correct treatment of personal information as very important to its successful operations and to maintaining confidence between the Association and those with whom it carries out business. The Association will ensure that it treats personal information lawfully and correctly.

To this end the Association fully endorses and adheres to the Principles of Data Protection as set out in the Data Protection Act 2018.

## 3. The principles of data protection

The Act stipulates that anyone processing personal data must comply with Eight Principles of good practice. These Principles are legally enforceable. The Principles require that personal information:

- Shall be processed fairly and lawfully and in particular, shall not be processed unless specific conditions are met;

- Shall be obtained only for one or more specified and lawful purposes and shall not be further processed in any manner incompatible with that purpose or those purposes;
- Shall be adequate, relevant and not excessive in relation to the purpose or purposes for which it is processed;
- Shall be accurate and where necessary, kept up to date;
- Shall not be kept for longer than is necessary for that purpose or those purposes;
- Shall be processed in accordance with the rights of data subjects under the Act;
- Shall be kept secure i.e. protected by an appropriate degree of security;
- Shall not be transferred to a country or territory outside the European Economic Area, unless that country or territory ensures an adequate level of data protection.

The Act provides conditions for the processing of any personal data. Personal data only includes information relating to natural persons who:

- can be identified or who are identifiable, directly from the information in question; or
- who can be indirectly identified from that information in combination with other information.

Special category data is personal data which GDPR says is more sensitive and so specific condition needs to be identified in order to process it. Special category data includes information about an individual's:

- Racial or ethnic origin;
- Political opinion;
- Religious or other beliefs;
- Trade union membership;
- Physical or mental health or condition;
- Sexual life or sexual orientation;
- Genetics or biometrics (where used for ID purposes);
- Criminal proceedings or convictions.

#### **4. Handling of personal/special category information**

The Regional Studies Association will, through appropriate management and the use of strict criteria and controls:-

- Observe fully conditions regarding the fair collection and use of personal information;
- Meet its legal obligations to specify the purpose for which information is used;
- Collect and process appropriate information and only to the extent that it is needed to fulfil operational needs or to comply with any legal requirements;
- Ensure the quality of information used;
- Apply strict checks to determine the length of time information is held;
- Take appropriate technical and organisational security measures to safeguard personal information;
- Ensure that personal information is not transferred abroad without suitable safeguards;
- Ensure that the rights of people about whom the information is held can be fully exercised under the Act.

These include:

- The right to be informed that processing is being undertaken;
- The right of access to one's personal information within the statutory 40 days;
- The right to correct, rectify, block or erase information regarded as wrong information.
- The right to object to and prevent processing in certain circumstances;
- The right to obtain and reuse personal data for their own purposes across different services.

In addition, the Association will ensure that:

- There is someone with specific responsibility for data protection in the organisation (Judy Pepper)
- Everyone managing and handling personal information understands that they are contractually responsible for following good data protection practice;
- Everyone managing and handling personal information is appropriately trained to do so;
- Everyone managing and handling personal information is appropriately supervised;
- Anyone wanting to make enquiries about handling personal information, whether a member of staff or a member of the Association, knows what to do;
- Queries about handling personal information are promptly and courteously dealt with;
- Methods of handling personal information are assessed and evaluated;

- Performance with handling personal information is assessed and evaluated;
- Data sharing is carried out under a written agreement, setting out the scope and limits of the sharing. Any disclosure of personal data will be in compliance with approved procedures.

All elected Board Members are to be made fully aware of this policy and of their duties and responsibilities under the Act.

All staff of the Association will take steps to ensure that personal data is kept secure at all times against unauthorised or unlawful loss or disclosure and in particular will ensure that:

- Paper files and other records or documents containing personal/sensitive data are kept in a secure environment;
- Personal data held on computers and computer systems is protected by the use of secure passwords, which where possible have forced changes periodically;
- Individual passwords should be such that they are not easily compromised.

All contractors, consultants, partners or other servants or agents of the Association must:

- Ensure that they and all of their staff who have access to personal data held or processed for or on behalf of the Association, are aware of this policy and are fully trained in and are aware of their duties and responsibilities under the Act. Any breach of any provision of the Act will be deemed as being a breach of any contract between the Association and that individual, company, partner or firm;
- Allow data protection audits by the Association of data held on its behalf (if requested).

All contractors who are users of personal information supplied by the Association will be required to confirm that they will abide by the requirements of the Act with regard to information supplied by the Association.

## **5. Implementation**

The Information Officer will also have overall responsibility for:

- The provision of data protection training, for staff within the Association.
- For the development of best practice guidelines.
- For carrying out compliance checks to ensure adherence, throughout the Association, with the Data Protection Act.

## **6. Notification to the Information Commissioner**

The Information Commissioner maintains a public register of data controllers. The Association is not currently required to be registered with the Information Commissioner, but this position will be checked from time to time.

## **7. Privacy/Personal Information Management**

The Regional Studies Association must ensure that both Board Members' and employees' personal data are kept confidential and made available only to authorised people for justifiable reasons.

It is necessary for the Association to retain some personal information on both Board Members and employees for statutory filing and personnel record and management reasons.

### *7.1 RSA Employees*

Personnel records are kept by the line manager and the CEO in the following ways:

- In the RSA staff folder where they are password protected;
- In locked filing cabinets for printed versions.

Personal information such as dates of birth are provided only to members of the RSA Staffing Sub-Committee unless other members of the RSA Board need to discuss issues which would necessitate them having access to this information.

### *7.2 RSA Board members*

The Association requires personal data from its Board Members for the Charity Commission as well as Companies House. This data will be retained by the CEO and the Finance Officer in order to facilitate statutory filing. The data will be kept in locked filing cabinets.

This policy will be reviewed annually.

---