

## RSA Academy Data Policy

This policy explains how The RSA Academy manages personal data of its staff and learners. It demonstrates how The RSA Academy complies with the Data Protection Act 2018 (DPA 2018) and the General Data Protection Regulation (GDPR) which is regulated by the Information Commissioner's Office (ICO) and how adherence to those requirements ensures the confidentiality of data.

### Scope of policy

This policy applies to all The RSA Academy staff and learners who use or process personal data. This policy applies regardless of where personal data is held and or the equipment used if the processing is for the RSA Academy's purposes. Further, the policy applies to all personal data, sensitive personal data or special category data held in any form whether paper or electronic records.

### General principles

The RSA Academy complies with the principles of good information handling, including:

- Processing personal data fairly and lawfully.
- Processing only as much information as we need to carry out the RSA Academy's activities. This will include course booking, eligibility for attending courses, payment details, course assessment and feedback, qualification registration.
- Taking reasonable steps to ensure personal data is accurate and current.
- Keeping personal data only for as long as is necessary.
- Keeping personal data securely and not passing it to anyone outside the RSA Academy without just cause.
- Not transferring personal data without adequate protection.

### Sensitive personal data or special category data

Will only occur when:

- The data subject has given consent to the processing of their sensitive personal data or special category data, *and*
- Processing the data is necessary to enable The RSA Academy to:

- a) conduct its activities, *or*
- b) protect interests of data subject, *or*
- c) comply with awarding organisation requirements

### **Communication**

This policy will be communicated to all tutor/assessors and the quality assurance team of the RSA Academy.

### **Roles and responsibilities - Senior management**

The Head of Centre and Academy Lead are responsible implementing this policy

### **Data Protection Officer**

The Academy Lead will act as Data Protection Officer (DPO) and is responsible for:

- compliance with the DPA and GDPR
- compliance with this policy
- detecting, investigating and reporting a breach of personal data
- primary point of contact for DPA and GDPR
- reviewing this policy

### **Employees and Data Processors**

All tutor/assessors and Data Processors must comply with this policy whenever processing personal data held by The RSA Academy.

### **Information we hold - Principles underpinning the information we hold**

The RSA Academy will only store personal data necessary to enable it to conduct its business. We will only hold Sensitive Personal Data when there is a clear requirement e.g. employee's health details and information necessary to assess eligibility for reasonable adjustments<sup>1</sup> for students.

### **Data Processors**

Generally The RSA Academy will not share Personal Data with third parties unless certain safeguards and contractual arrangements have been put in place. The RSA Academy will share the Personal Data

we hold with 3<sup>rd</sup> parties such as awarding organisations and learners' employer if the recipient has a job-related or a service related need to know the information.

Personal data we hold for employment and service delivery purposes may include:

- Full name and title
- Personal email address
- Personal telephone number/s
- Emergency contact details

### **Learners**

Personal data we hold for The RSA Academy's purposes only:

- Employers and co-ordinators contact details
- Contact details e.g. email address and telephone numbers
- Information to determine eligibility for attending courses
- Payment history and details

Personal data we hold for educational reasons and share with awarding organisations:

- Full name and title
- Gender
- Date of birth
- Identity information e.g. UK address, photo ID: e.g. driving licence or passport

Personal data we hold for educational reasons and may share with awarding bodies:

- Information included in evidence submissions
- Reasonable adjustments, qualification registration, appeals, malpractice allegations, complaints and investigations associated with educational matters

### **Processing personal data - Principles of processing personal data**

The processing of personal data will only be carried out where one of the following conditions has been met:

- The individual (Data Subject) has given their consent
- It is necessary for the performance of a contract with the individual
- A legal obligation exists
- It is in the individual's interest
- It is necessary for the administration of justice
- The benefits are for the legitimate interests of the company and do not outweigh any detriment to the individual

### **Confidentiality**

- Any information provided to The RSA Academy will remain confidential and only be used for the purposes for which it has been disclosed.
- Unless The RSA Academy has permission, we will not sell, distribute or lease personal and confidential information to third parties, unless we are required by law to do so.

### **Data Subjects rights**

With regards to the personal data we store, data subjects have rights to:

- **Receive a copy** of the personal information we hold about them and that we are lawfully processing their data
- **Request correction** of the personal information that we hold about them.
- **Request erasure** of their personal information. This enables them to ask us to delete or remove personal information where there is no justification for us continuing to process it.
- **Object to processing** of their personal information where we are relying on a legitimate interest (or those of a third party) and there is something about their particular situation which makes them want to object to processing on this ground. They also have the right to object where we are processing their personal information for direct marketing purposes.
- **Object to automated decision-making including profiling**, that is not to be subject of any automated decision-making by us using their personal information or profiling of them.
- **Request restriction of processing** of their personal information. This enables them to ask us to suspend the processing of personal information about them, for example if they want us to establish its accuracy or the reason for processing it.

- **Request transfer** of their personal information in an electronic and structured form to them or to another party (commonly known as a right to “data portability”). This enables them to take their data from us in an electronically useable format and to be able to transfer their data to another party in an electronically useable format.
- **Withdraw consent.** In the limited circumstances where they may have provided their consent to the collection, processing and transfer of their personal information for a specific purpose, they have the right to withdraw their consent for that specific processing at any time. Once we have received notification that they have withdrawn their consent, we will no longer process their information for the purpose or purposes they originally agreed to, unless we have another legitimate basis for doing so in law.

### **Consent for processing activities**

We normally only process personal data for the following activities:

- Record keeping e.g. courses attended, dietary requirements, reasonable adjustments etc.
- Qualification registration
- Notification of course/RPL assessments, re-submission requirements etc.
- Posting of certificates and evidence submissions
- Expression of interest in the services The RSA Academy provide
- Marketing for activities in which organisations and individuals have shown an interest
- Taking credit and debit card payments.

### **Data subject access requests**

Individuals can submit a written email request to [academy@residentialsprinklerassociation.org.uk](mailto:academy@residentialsprinklerassociation.org.uk) regarding what personal information is held about them, how it is processed and the circumstances in which it is disclosed.

This will normally be completed free of charge and be dealt with within one month of the request.

Should the request be manifestly unfounded, excessive or repetitive then we may refuse or charge for responding.

If we refuse a request, we will inform you why your request has been refused. If this occurs you have a right to complain to the supervisory authority and to a judicial remedy.

## **Data Protection - Principles of data protection**

To prevent unauthorised access or disclosure of personal data, we have put in place suitable physical, electronic and managerial procedures to safeguard and secure the information we collect.

## **Responsibilities**

The Data Protection Officer is responsible for the security of electronic and hard copies of personal data.

## **Data Processor responsibilities**

Data Processors are responsible to:

- manage personal information to which they have access e.g. each employee and Data Processor is responsible for the information they access, receive, store, use, disclose and process.
- ensure that personal information is kept secure at all times and is not disclosed to unauthorised persons.
- ensure that any locked stores remain locked and keys kept secure.
- keep IT password/s secure. See password policy detailed in IT Systems Policy

## **Access to personal data**

- Access to information will be restricted to authorised personnel only.
- Each authorised person will be restricted to accessing information relevant to the areas necessary to carry out their role.
- The Administration Manager is responsible for identifying the level of access for each employee.

## **Hard/paper based records**

- Paper records with personal information are kept in a locked store.
- Access is only available to authorised personnel.
- Personal information will only be disclosed to those who require access to carry out their roles and for the purposes for which it was provided e.g. assessment, qualification registration, investigation etc.

- When the information is no longer required, it will either be returned to the person concerned, shredded or archived in a secure area.

### **Electronic information**

- Electronic information is stored in a secure area on the RSA's SharePoint and Vault.
- Access is password protected.
- Access is only available to authorised personnel.

### **Retention & Disposal of personnel data**

The RSA Academy will ensure Personal Data is destroyed after a reasonable time for the purposes for which it was being held, unless a law requires that data to be kept for a minimum time.

Personal information no longer required will be disposed in following manner:

- Personnel information stored on paper will be shredded before disposal.
- Personnel information stored electronically will be wiped.

### **IT Security**

#### **Principles of IT Security**

The RSA Academy has systems designed to achieve the following objectives:

- Comply with business IT best practice
- Store information in an efficient manner
- Prevent unauthorised access

#### **Data Breaches - Data Breach**

Any employee, Data Processor, student or supplier who knows or suspect an actual or potential personal data breach has occurred must immediately notify the Data Controller by email:

[academy@residentialsprinklerassociation.org.uk](mailto:academy@residentialsprinklerassociation.org.uk)

All RSA Academy staff are responsible for fully engaging and cooperating with the Data Controller in relation to an investigation of a personal data breach.

## Response

The RSA Academy will respond promptly to any identified personal data breaches and thoroughly investigate those incidents to ascertain whether:

- Data subjects should or must be made aware of the breach; *and*
- It is necessary to amend processes or introduce new measures to mitigate against any further breaches.

For Review August 2025