The Royal Institution
Science Lives Here

Data Protection policy

STATUS: Approved

Policy Effective Date: 05 March 2024

Policy Owner: Director of Finance & Resources

Date approved: 06 March2024

Next Review Date: February 2026

1 Purpose

1.1. The purpose of this policy is to assist the Royal Institution ('the Ri') in meeting its legal obligations under data protection legislation. It describes the responsibilities of everyone working for, and representing the Ri, whether employee, contractor, or volunteer, and the rights of access by individuals to their personal data.

2 Scope

2.1 The Ri processes personal information of its staff, volunteers, representatives, members, patrons, beneficiaries, and other individuals (such as key business contacts). Personal information is kept in a range of forms, including the following:

a) Digital records
b) Paper records
c) Video footage
d) Audio recordings
e) Photographic material

2.1. This policy should be read in conjunction with, but not limited to:

a) The Data Protection Procedure
b) The Computer Acceptable Use Policy
c) Bring Your Own Device Acceptable Use Policy

3 Context

3.1. The Royal Institution of Great Britain ('the Ri') is a Data Controller under the Data Protection Act 2018 (DPA 2018), the UK General Data Protection Regulations (UK GDPR) and The Privacy and Electronic Communications Regulations (PECR), together referred to in this policy as 'the data protection legislation.' As such the Ri have notified the Information Commissioner's Office (ICO), the body responsible for ensuring data protection compliance in the UK and are registered on the Data Protection Register - registration number Z7087010. RiGB Ltd is the wholly owned trading subsidiary of the Ri, registered company No: 04065626. In this policy references to "the Ri" or "we" are to the Royal Institution of Great Britain charity and to its trading subsidiary company RiGB Ltd.

3.2. For details of the legislation please see Information Commissioner's Office (ICO) website ico.org.uk

4 Governance and Responsibilities

4.1. The Trustees are responsible for determining this policy.

4.2. The Audit and Risk Committee are responsible for review of this policy.

4.3. Our Data Protection Officer, named at the ICO, is the Director of Finance and Resources. Some duties are delegated to members of the Data Protection Group:

- Head of IT
- Membership Manager
- Manger of Governance and Risk

4.4. The Data Protection Group are responsible for management of data protection incidents, review of the policy and providing information about the policy within the Ri.

4.5. The executive and senior leadership team are responsible disseminating the policy and linked procedures.

4.6. All staff are responsible for understanding and adhering to this policy.

5 Policy statement

5.1. The Ri ensures that personal information is collected and processed in line with the six principles of the data protection legislation. Article 5 of the UK GDPR states that personal data must be:

5.1.1. processed lawfully, fairly and in a transparent manner in relation to individuals;

5.1.2. collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be incompatible with the initial purposes;

5.1.3. adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed;

5.1.4. accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified;

5.1.5. 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; personal data may be stored for long periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes, subject to implementation of the appropriate technical and organisational measures required by UK GDPR in order to safeguard the rights and freedoms of individuals; and

5.1.6. 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.

6 Policy - it is our policy to ensure that:

6.1 appropriate structures are in place to ensure that there is a chain of responsibility for data protection within the organisation.

6.2 data subjects are informed that the Ri is a registered organisation that collects certain data for specific purposes and on pre-defined lawful bases, through data

processing statements (privacy notices and privacy policy).

6.3 data processing notices must be clear and easy to understand, explain the purposes for which and the lawful bases on which the personal data will be processed.

6.4 transparency is maintained in how the information is collected and how it will be used.

6.5 only necessary data is processed and that it is only used for the purposes of the original collection.

6.6 data will not be retained once it is no longer required for its stated purpose.

6.7 data is not processed in a way that would have unjustified adverse effects on the data subject, or for unlawful purposes.

6.8 all staff, contractors, volunteers and representatives that have access to or process personal data understand that they are required to abide by this policy, and the data protection legislation.

6.9 staff contractors, volunteers and representatives receive the necessary training and access to information they need to be able to adhere to the requirements of the data protection legislation and to prevent as far as possible unintentional data breaches.

6.10 appropriate disciplinary procedures will be enforced in situations where the data protection legislation is knowingly breached by staff, or by other data controllers and/or data processors the Ri has contracts with.

6.11 appropriate measures are in place to limit personal data breaches. If a breach does occur, in line with the legislation, the Ri will report the breach to the relevant supervisory authority within the 72-hour guidelines. If the breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms, the Ri will inform those individuals without undue delay. In line with UK GDPR the Ri will keep a record of any personal data breaches, regardless of whether we are required to notify or not.

6.12 As an organisation that regularly collects personal data from young people for specified purposes, staff recognise their responsibility to obtain the correct consent from an individual with appropriate authority. The law permits those aged 13-18 years of age to give consent. Ri policy is to gain parental consent for all those aged 16 years and under. Directors may exceptionally agree to deviate from this policy but must take into account the specific circumstances, type of data and risks to children before doing so. Parental consent or consent from those acting in a parental capacity (e.g., carer, teacher) must always be obtained for every child under 13 years of age.

6.13 **Subject access requests:** Requests received from individuals for a copy of the information the Ri holds on them will be passed to the Ri Data Protection Officer for processing. Subject access requests for personal information need to be made in writing with sufficient supporting evidence to validate the individual's identity to the Ri's satisfaction, and to be able to identify what information is being requested. Requests will be responded to within one month of the date all the information required to be able to fulfil the request is received.

6.14 **Freedom of Information Request:** As a registered charity the Ri is not directly subject to the Freedom of Information Act 2000. Separate guidance exists for Freedom of Information requests and must be consulted before any response is offered to the request.

7 Relevant/ linked policies, procedures or forms

7.1 Data Protection at the Ri – Guide for staff

7.2 Data protection personal data map

7.3 Data Protection DPIA template

7.4 Information Commissioners Office (ICO) website https://ico.org.uk

7.5 Safeguarding Policy

7.6 Computer Acceptable Use Policy

7.7 Bring Your Own Device (BYOD) Policy

7.8 Data Protection Group Terms of Reference

7.9 Disciplinary Policy

8 Monitoring, reporting requirements, review and/or enforcement

8.1 Suspected data breaches are reported as per the Data Protection procedure.

8.2 Data breaches are reported to the ICO within the 72 hour framework as defined by the ICO.

8.3 All Data Breaches must be declared to Audit and Risk Committee.

8.4 Subject access requests are reported as per the Data Protection procedure.

8.5 Subject access requests are processed in accordance with the Data protection procedure.

8.6 Relevant assurance frameworks departmentally embed data protection at their heart. These include IT security practices and software designed to prevent and/or limit data breaches.

8.7 Awareness and training for staff members is undertaken.

8.8 Project management data protection impact assessments (DPIAs) enforced.

8.9 Lawful basis for processing register maintained.

9 Definitions

9.1 "**the Ri**" or "**we**" are to the Royal Institution of Great Britain charity and its trading company RiGB Ltd.

9.2 **Data Protection legislation**
For the purposes of this document this is the Data Protection Act 2018 (DPA 2018), the UK General Data Protection Regulation (UK GDPR) and The Privacy and Electronic Communications Regulation (PECR), together referred to in this policy as 'data protection legislation'.

9.3 **GDPR or UK GDPR**
This stands for General Data Protection Regulations (GDPR), the EU's agreed

standards for data protection that are written into UK law through the Data Protection Act 2018 (DPA 2018). GDPR was retained in UK law as UK GDPR and will continue to be read alongside the DPA 2018.

9.4 **Personal information**

Personal data is information about who you are, where you live, what you do and more. Any and all information that identifies a living individual a data subject. There are a few examples below, the list is not exhaustive.

- people's names and addresses
- photographs
- customer reference numbers
- medical information
- school reports; and
- customer reviews

9.4.1 If a document, file, or image identifies a person, or could be used in combination with other information to identify them, then it's personal data. This applies even if the information does not include a person's name.

9.5 **Data controller**

A data controller has the responsibility of deciding how personal data is processed and protecting it from harm. For the purposes of this policy that is the Ri.

9.6 **Data subject**

A data subject is someone who can be identified from personal data. The data could be their name, address, telephone number or something else – but if it is about a person, then they are the data subject. They are the 'subject' of the data. However, the term only relates to people who are alive. Data protection law does not apply after someone has died. At the Ri this may be but not limited to members, patrons, staff, volunteers, beneficiaries, contacts.

9.7 **Data processing**

In a similar way to data controllers, data processors must protect people's personal data – but they only process it in the first place on behalf of the controller. They would not have any reason to have the data if the controller had not asked them to do something with it.

9.8 **Data breach**

If any personal data that the Ri is responsible for has been lost, accidentally destroyed, altered without proper permission, damaged, or disclosed to someone it should not have been, this may be a personal data breach. Decisions on what constitutes a data breach can be found at ico.org.uk/for-organisations/report-a-breach/.

9.9 **Lawful basis**

A lawful basis is the reason or legal grounds you can rely on for using people's personal data. There are six bases:

a) consent
b) contract
c) legal obligation
d) vital interests
e) public task
f) legitimate interest