# Section 6.1

# DATA PROTECTION POLICY

## Policy Statement

RBGE collects and uses information about people, including:

* Staff, volunteers and applicants for jobs and voluntary posts;
* Supporters, visitors, donors and enquirers;
* Students and researchers.

This personal information will be managed appropriately and securely - however it is collected, recorded and used, whether on paper or digitally– in compliance with the Data Protection Act 2018 (DPA) and the General Data Protection Regulation (GDPR).

The purpose of this policy is to ensure that RBGE has robust procedures in place for demonstrable compliance with GDPR/DPA.

## Principles

Data users must comply with the data protection principles. Whenever RBGE works with personal data it will be:

1. processed fairly, lawfully and transparently (see [RBGE Privacy Notice](http://www.rbge.org.uk/privacy-notice))
2. collected for specific purposes and not used for incompatible purposes
3. adequate, relevant and limited to what is necessary
4. accurate and, where necessary, kept up to date
5. retained no longer than necessary (see [RBGE Records Retention Schedule](http://greenpages.rbge.org.uk/using-services/records-management?searched=retention+schedule&advsearch=allwords&highlight=ajaxSearch_highlight+ajaxSearch_highlight1+ajaxSearch_highlight2))
6. kept securely (see RBGE Information Security Policy)

The principles apply to “personal data” - any information from which an individual is identifiable.

RBGE staff and volunteers who process or use any personal information in the course of their duties must ensure that these principles are followed at all times.

## Responsibilities

The **Head of Resources and Planning** has specific senior responsibility for data protection within RBGE.

**Information Asset Owners (IAOs)** are senior/responsible individuals involved in running a relevant business area. Their main responsibility is to ensure that the information asset is managed appropriately to meet the requirements of the organisation and that risks and opportunities are monitored. Examples of IAO)’s include the Head of HR, the head of Finance, the Head of Education, the Director of Enterprise and Communication and the Director of Science.

Each **(IAO)** has responsibility for ensuring that the information under their control is collected, processed and held in accordance with this policy and the GDPR and that there is a current accurate description of all information assets for which they are accountable in the RBGE Information Asset Register.

The **Data Protection Officer** (DPO) is responsible for advising on and monitoring RBGE’s compliance with GDPR and providing a point of contact for data subjects and the Information Commissioner’s Office **(ICO).** The RBGE DPO is currently Jane McCrorie, HR Projects Manager.

**All** RBGE staff, volunteers and any contractors or agents performing work for or on behalf of RBGE and any other individuals with access to RBGE’s information have a responsibility to ensure that personal information is properly protected at all times. This includes using personal data only within their authorised role and in compliance with this policy and other ICT and Information Security policies. Adherence to data protection policy and procedures, as with other RBGE policies, is required to comply with the law in this area.

**All** RBGE staff, volunteers and any contractors or agents performing work for or on behalf of RBGE have a responsibility to report to the DPO any observed or suspected incidents threatening the confidentiality, integrity or availability of personal data held by RBGE.

## Processing personal data at RBGE

RBGE collects and uses personal data for a variety of reasons:

* Recruitment and selection
* Administration of contracts of employment e.g. salaries and allowances, pensions and associated benefits, appraisal, training and development, compliance with statutory requirements
* Financial information (e.g. bank account details and credit card information)
* Health and safety
* Management of volunteers
* Management of students
* Marketing, promotion and fundraising
* Collections information (e.g. donors, vendors, loans)
* Identification purposes, such as library user records, staff photographs
* Membership records, contacts, databases and mailing lists
* Contacts for collaborative research

Staff, volunteers and contractors working under the auspices of RBGE must only access or use personal data held by or within RBGE in accordance with this policy and for specific authorised purposes. All staff must keep network usernames and passwords secure and use information systems in line with the appropriate procedures and training.

## Retention of Data

Personal data must not be retained for longer than is necessary. RBGE IAO’s and managers are responsible for ensuring that the Record Retention Schedule is applied to all records and documents holding personal data, by having regular or automated deletion or destruction of personal data in systems, paper files and on network folders.

All documents containing personal data should be disposed of securely in accordance with the Data Protection principles.

## Transfer of Personal Data

Any mobile device or digital media (such as a laptop, mobile phone, tablet or USB memory device) holding personal data or used for processing RBGE personal data, (whether that device is RBGE or privately owned) must be encrypted. Further guidance for staff can be found in [Green Pages](http://greenpages.rbge.org.uk/using-services/ict-services/using-desktop-computing/saving-and-storing-documents/using-a-secure-usb-memory-device).

If you need to send personal information by email then please read the guidance on protecting documents for sending by email on [Green Pages](http://greenpages.rbge.org.uk/using-services/ict-services/using-desktop-computing/using-e-mail/protecting-documents-for-sending-by-e-mail?searched=protecting+documents&advsearch=allwords&highlight=ajaxSearch_highlight+ajaxSearch_highlight1+ajaxSearch_highlight2).

## Personal data rights

RBGE will ensure individuals’ rights are respected with regard to their personal data. Rights under GDPR include:

* the right to be informed that processing is being undertaken (GDPR art 13 and 14);
* the right of access to one's own personal data and to specific information about the processing (GDPR art 15);
* the right to object to and prevent processing in certain circumstances (GDPR art 21);
* the right to rectify or restrict inaccurate data (GDPR art 16 and 18);
* the right to erase data or to data portability in certain circumstances (GDPR art 17 and 20).

All requests relating to GDPR rights should be directed to the DPO.

## Personal data incidents and breaches

Any incident which may impact on the confidentiality, integrity or availability of personal data held by RBGE should be reported immediately to the DPO. Such incidents could include events such as:

* Loss of RBGE records, laptops or media;
* Unauthorised access to RBGE information systems;
* Personal data being misdirected to an incorrect recipient.

The DPO will record the incident, ensure appropriate mitigation measures are put in place and consider whether the incident meets the GDPR definition of a personal data breach which presents a risk to individuals.

The DPO will present a report to the Head of Resources and Planning including, if appropriate, a recommendation on whether to report a breach to the ICO within 72 hours of RBGE becoming aware of the incident.

If the Head of Resources and Planning concludes that an incident constitutes a reportable breach, the DPO will report the incident to the ICO and liaise as appropriate.

## Governance of Data Protection

RBGE will maintain robust oversight and transparency in the management of personal data. We will meet our record-keeping duties through the maintenance of:

* Up-to-date **privacy notice information** (see article 13 and 14 of GDPR);
* An **Information Asset Register** describing the content, purpose, controls and the RBGE staff member with accountability for each data system or set of records holding personal data;
* A **log of information security incidents**;
* The RBGE **Information Security policy**.

RBGE will apply **Privacy By Design** principles for new systems and business processes. This means that privacy and data protection will be a key consideration in the early stages of any project, and then throughout its lifecycle. Taking a privacy by design approach will help minimise privacy risks and will build trust. As appropriate, the relevant Information Asset Owner may be asked to complete a Data Protection Impact Assessment in line with a template and guidance from the ICO.

All contracts with organisations processing personal data on behalf of RBGE (**data processors**) will have GDPR-compliant contract clauses and be subject to appropriate levels of review and oversight.

All RBGE staff and volunteers will receive training and awareness-raising on data protection and information security relevant to their role.

For personal data processed for electronic **direct marketing** purposes (newsletters and other promotional materials sent by email or text message) RBGE will only use contact details for private individuals where they have explicitly opted-in (consented) to receive such communications from RBGE.

Policy approved date: May 2018

Policy review date: May2020