POLICY

Data Handling Policy

Date: 25 May 2018

This document defines the Data Protection Policy at the Royal Society of Biology and offers guidance on duties and best practice to users. This document contains the following sections:

- Introduction
- Definitions
- Scope of this policy
- Principles of data handling
- Handling sensitive data
- Sending data to third parties
- Addressing data handling in contracts and agreements
- Taking data away
- Handling Subject Access Requests
- Privacy Policy
- Law Enforcement Requests & Disclosures
- Location and Transfer of data
- Training related to Data Protection, Privacy and Handling
- Notification in case of breach or for other reasons
- Automated Decision Making and Profiling
- Sending bulk email and mail merge communications
- Related Documents
- Contact Information

Introduction

The Royal Society of Biology handles a substantial amount of data in order to pursue its mission and vision. Much of this data is private and/or personal data, some is sensitive. When handling the Society's data, of any kind, you must always act in accordance with this policy.

Definitions

For the purpose of this policy, the following definitions apply:

Personal data: any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier (including name, email address, IP address, identification number, location data etc).

Sensitive data: any data related to racial or ethnic origin, political opinions, religious/philosophical beliefs, trade union membership, genetic data, biometric data,

health data, sex life or sexual orientation, bank account details, debit or credit card details and any data related to children and minors under the age of 13.

Other data: any data that is not personal data or sensitive data.

Scope of this policy

This policy applies to all forms of data handling at the Royal Society of Biology or on its behalf, manual or automated, in paper, electronic or any other form and to all categories of data without limitation.

Principles of data handling

When handling any data at the Royal Society of Biology, you should always operate within the following principles:

Principle 1: Lawfulness, Fairness and Transparency

All data at the Royal Society of Biology shall be processed lawfully and fairly. Where personal data, including sensitive data, is handled, this shall also be done in a manner transparent to the identified or identifiable person to which the data refers.

There must at all times exist a legal basis as defined in the General Data Protection Regulation (GDPR) for the collecting, storing and processing of all data. If in doubt, you must consult with the Data Protection Officer.

Principle 2: Purpose Limitation and Relevance

Data at the Royal Society of Biology is collected for specified, explicit and legitimate purposes in accordance with the Society's mission and vision. This data is never processed in a manner that is incompatible with those purposes. This means that when collecting and/or processing data, you should always specify exactly what the data will be used for and limit any handling and processing to only what is necessary to meet the specified purpose.

Where the purpose for processing data is no longer valid or there no longer exists a valid legal basis for it, the data must be securely deleted.

Principle 3: Accuracy

You should at all times take every reasonable step to ensure that data is accurate and kept up to date. Where data is known to be wrong, it should be rectified without delay. If you are unable to correct the data, you should report any inaccuracies with the aim to get it amended.

Principle 4: Personal and sensitive data is held on MARVIN

Unless explicitly allowed by either the IT Director or the Chief Executive, all personal data and all sensitive data must be held and processed on MARVIN, the Royal Society of Biology's central database.

Principle 5: Storage Limitation and Retention

Personal and sensitive data shall be kept for no longer than necessary for the purpose for which the data is collected, stored and processed. Where possible, data that is retained for historic, statistical or other relevant purposes should be anonymised as much as possible.

Principle 6: Security, Integrity and Confidentiality

All data at the Royal Society of Biology should be handled, at all times, in a manner that is secure and that maintains the data's integrity and confidentiality. All necessary precautions must be taken to protect against unauthorised or unlawful processing, against accidental loss, destruction or damage and against theft.

Handling sensitive data

You must not, under any circumstance, collect, store, access or process sensitive data unless you have been authorised to do by the Chief Executive, the Data Protection Officer or the IT Director.

Sending data to third parties

Sharing data with third parties must only be done where strictly necessary, in a way that is secure, lawful and fair and with the explicit approval of either the IT Director, the Data Protection Officer or the Chief Executive.

Wherever data is transmitted to third parties, this must always be done using an approved method. Unless not possible for good reason, data should be communicated by direct file upload or other appropriate form of electronic transmission.

Removable media (including USB sticks, external hard drives, CD, DVD, etc) other than the Royal Society of Biology's approved encrypted USB sticks **must not be used** for transmitting data to third parties, unless approved by the IT Director.

Addressing data handling in contracts and agreements

Managers and other staff responsible for contracts/agreements with third party joint-controllers or data processors must ensure that contracts include appropriate provisions to ensure compliance with the law and with this data handling policy. This must include provisions addressing:

- adherence to the principles as set out above;
- mutual notification of breaches;
- ensuring at all times adequate security of all personal data;
- handling of subject access requests in a timely and complete manner and ensuring that requests received by a third party are passed on to the Royal Society of Biology without delay.

Taking data away

Where you download, copy or otherwise handle data outside of the Royal Society of Biology's office, you must take all appropriate measures to ensure this data remains secure and is not shared, exposed or otherwise compromised in any way. Such data should never be left unsupervised and should never be left behind. Where the data or copy is no longer needed for the purpose for which it was obtained, it must be deleted or disposed of in a secure manner.

Handling Subject Access Requests

Where a person makes a request ("subject access request") in relation to their personal data, exercising their legal right to:

- Access the information we hold on them ("right of access");
- Request we rectify information we hold ("right to rectification");
- Request we delete their information ("right to erasure");
- Suppress or limit processing of personal data ("right to restrict processing");
- Move, copy or transfer their personal data ("right to data portability");
- Object against processing of their data ("right to object");
- Query or object against automated decision making and profiling ("right on automated decision making");
- Withdraw their consent to process personal data;

such request must without delay be handed over to the Data Protection Officer or the IT Director and handled in compliance with legal obligations and internal procedure (see "Procedures - Subject Access Requests").

Where you are involved in handling personal data that is relevant to any such subject access request, you must respond immediately to any requests from the Data Protection Officer or the IT Director in relation to their handling of the subject access request.

The document "Procedures - Subject Access Requests" provides more detail about how subject access requests are to be handled.

Privacy Policy

All the websites of the Royal Society of Biology will include a link to our Privacy Policy. You must read and understand this Policy. When asked, you should point people to our Privacy Policy for guidance.

https://my.rsb.org.uk/item.php?privacy=policy

Law Enforcement Requests & Disclosures

Where disclosure of personal data is required:

- to prevent or detect crime;
- to apprehend or prosecute offenders;

- by the order of a court or by any rule of law.

you must immediately inform the Data Protection Officer or the IT Director so that the situation can be handled in compliance with legal obligations and internal procedure.

Location and Transfer of data

It is the policy of the Royal Society of Biology to store, process and handle all data within the European Union.

Wherever data is transferred outside of the European Union, this is only permitted:

- to a country that has been deemed to provide an adequate level of protection by the European Commission;
- by using specific contracts approved by the European Commission which give personal information the same protection it has in the European Union;
- to the US, on condition that the US based provider is part to contract or legal obligation to provide similar protection to personal data it has in the European Union.

No data must be transferred outside the European Union without explicit approval of either the IT Director, the Data Protection Officer or the Chief Executive.

Training related to Data Protection, Privacy and Handling

All employees, contractors and volunteers that have access to personal data must be made aware of this policy and of the Privacy Policy published on our website at the start of their employment or involvement and attend a data protection training session within one month of the start of their employment or involvement. Line managers must ensure compliance with the policy at all times.

Notification in case of breach or for other reasons

If you become aware that any data has been breached, leaked, has been stolen or lost or is otherwise compromised, you should immediately report this to any of the contacts named below, at the end of the policy.

If you suspect that the cause is malware in any form, you should immediately cease any processing and shut down affected systems or devices.

More detail about handling of data breach incidents can be found in the Royal Society of Biology's "Incident Plan - Information Systems".

Automated Decision Making and Profiling

The Royal Society of Biology will not:

- make any decision about an individual solely by automated means without any human involvement;

- process personal data automatically (without human involvement) to evaluate certain things about an individual (profiling).

Sending bulk email and mail merge communications

MARVIN must be used for any bulk email or mail merge communication on behalf of the Royal Society of Biology, unless you have received written permission from the Chief Executive, the Data Protection Office or the IT Director to do otherwise.

This is because MARVIN provides tools to help to ensure that such communications are lawful and fair. Where MARVIN prompts you to select the appropriate legal basis for an action, you must select the correct basis at all times and not proceed until you have done so. If in doubt, seek advice from the Data Protection Officer.

Related Documents

- Procedures - Subject Access Requests
- User Guide - Password Policy & Guidance
- Incident Plan - Information Systems

Contact Information

If you need to report data breaches or security concerns or any other matter related to this policy, do this immediately and preferably face to face or over the phone (email or other messages may not be seen immediately):

Mark Leach (Data Protection Officer) – 020 3925 3446

Jennifer Crosk – 020 3925 3472

Ana Ilic - 020 3925 3473

If neither Mark, Jen nor Ana are available, please contact:

Guido Gybels (IT Director) – 077 6535 4408.