General Data Protection Policy

Document Date:	22 February 2022
Purpose:	To set out the organisational approach to the Data Protection Act 2018. The goal is to ensure we take a principle based approach to protecting individual's data and staff understand the responsibilities placed on individuals and the organisation. The document should be read in conjunction with the Privacy Policy.
Audience:	Permanent staff, casual staff, contractors.

1. Introduction

1.1 Royal Holloway Students' Union (RHSU) is committed to all aspects of data protection and takes seriously its duties, and the duties of its employees, under the Data Protection Act 2018 (UK GDPR). The purpose of this policy is to set out:

i. How the organisation deals with personal data relating to staff;
ii. The principles under which data will be processed by the organisation;
iii. And the expectation the organisation has on its staff in relation to their individual responsibilities regarding the processing of data.

1.2 This policy should be read in conjunction with the organisation's Privacy Policy, which specifically sets out how the organisation will use information collected in relation to its staff and members.

2. The Law

2.1 The Data Protection Act 2018 is the UK's implementation of the General Data Protection Regulation (GDPR) and replaced the Data Protection Act 1998.

2.2 It sets out the key principles, rights and obligations for most processing of personal data in the UK, except for law enforcement and intelligence agencies.

3. The Organisation's Responsibilities

3.1 RHSU is the Data Controller and is responsible for determining the purposes for which, and the manner in which, any personal data is processed.

3.2 The primary contact to the Information Commissioner's Office (ICO) is the Chief Executive, who is responsible for maintaining the annual notification to ICO.

3.3 The organisation has appointed a senior manager as the person with responsibility for data compliance within the organisation. This is the Head of Marketing and Communications, Michael Bailey, who can be contacted at michael.bailey@su.rhul.ac.uk.

3.4 Senior managers and line managers are responsible for ensuring this policy is observed within their teams. Anyone who collects, stores or uses personal data on behalf of the Students' Union must comply with the GDPR principles outlined below.

4. Individual Staff Responsibilities

3.5 Individuals whose role requires them to process personal data of other individuals (either staff or members) in the course of their employment, must comply with this policy.

3.6 Individuals who have access to personal data are required to:

- Access only data they have the authority to access and only for authorised purposes;
- Not disclose data except to individuals (whether inside or outside the organisation) who have appropriate authorisation;
- Keep data secure (for example by complying with rules on access to premises, computer access, including password protection, and secure file storage and destruction);
- Not to remove personal data, or devices containing or that can be used to access personal data, from the organisation's premises without adopting appropriate security measures (such as encryption or password protection) to secure the data and the device; and
- Not store personal data on local drives or on personal devices that are used for work purposes.

3.7 Staff who process personal data will be provided with GDPR training as part of their induction and any refresher training as required by their line manager.

3.8 Staff who commission or employ third parties to process personal data on behalf of, or in connection with, RHSU must ensure that the details of such processing are subject to a written agreement between RHSU and the third party.

3.9 Further guidance for staff can be found in the associated Guidance to GDPR for Employees.

4. Definitions

4.1 “Personal data” is any information that relates to an individual who can be identified from that information. Identified/identifiable means you can distinguish one individual from a group of others with the most common means being a name. The UK GDPR sets out a non-exhaustive list of identifiers including:

i. Name;
ii. Identification number e.g. Student ID number or an employee number;
iii. Location data e.g. an address on a database; and
iv. An online identifier e.g. a username to access one of our systems.

4.2 “Special category data” is personal data that needs more protection because it is sensitive. In order to process special category data a lawful basis under Article 6 of the UK GDPR and a separate condition for processing under Article 9 must be identified. The nine categories are:

i. Personal data revealing racial or ethnic origin;
ii. Personal data revealing political opinions;
iii. Personal data revealing religious or philosophical beliefs;
iv. Personal data revealing trade union membership;
v. Genetic data;
vi. Biometric data (where used for identification purposes);
vii. Data concerning health;
viii. Data concerning a person’s sex life; and
ix. Data concerning a person’s sexual orientation.

4.3 “Processing” is any use that is made of data, including collecting, storing, amending, disclosing or destroying it. There must be a valid lawful basis in order to process personal data from the six

available lawful bases. This basis needs to be determined before any processing of data takes place and recorded on our GDPR Audit Log.

5. Data protection principles

5.1 Under the GDPR, the data protection principles set out the main responsibilities for organisations. These principles require that personal data shall be:

i. Processed lawfully, fairly and in a transparent manner;
ii. Collected only for specified, explicit and legitimate purposes and not processed in a manner that is incompatible with those purposes;
iii. Adequate, relevant and limited to what is necessary in relation to the purposes of processing;
iv. Accurate and kept up to date, where necessary, with all reasonable steps taken to ensure that inaccurate data is rectified without delay;
v. Kept only for the period necessary for processing;
vi. Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing, and accidental loss, destruction or damage.

5.2 Note, these are separate to the lawful bases for processing and the individual rights.

6. Privacy Notices

6.1 RHSU tells individuals the reasons for processing their personal data, how it uses such data and the basis for processing the data in its various privacy notices. It will not process personal data of individuals for other reasons.

6.2 RHSU's central privacy notice is located on our website. Other, specific privacy notices will be issued at relevant stages of data collection (i.e. recruitment).

7. Individual Rights

7.1 As a data subject, individuals have a number of rights in relation to their personal data as follows:

7.2 <u>Subject Access Requests (SAR)</u>

i. Individuals have the right to make a subject access request. If an individual makes a subject access request, RHSU will tell them:

    a. Whether or not their data is processed and if so why, the categories of personal data concerned and the source of the data if it is not collected from the individual,
    b. To whom their data is or may be disclosed, including to recipients located outside the UK and the safeguards that apply to such transfers;
    c. For how long their personal data is stored (or how that period is decided);
    d. Their rights to rectification or erasure of data, or to restrict or object to processing;
    e. Their right to complain to the Information Commissioner's Office (ICO) if they think the organisation has failed to comply with their data protection rights; and
    f. Whether or not the organisation carries out automated decision-making and the logic involved in any such decision-making.

ii. The organisation will also provide the individual with a copy of the personal data undergoing processing. This will normally be in electronic form if the individual has made a request electronically, unless they agree otherwise.

iii. An individual can make a SAR verbally or in writing, including on social media. The request must be treated as valid if it is clear that the individual is asking for their own personal data. In some cases, we may need to ask for proof of identification before a request can be processed. For additional support, please read the Subject Access Request guide.

iv. The organisation will normally respond to a request within a period of one month from the date it is received. In some cases, such as where large amounts of the individual's data is being processed, it may respond within three months of the date the request is received. RHSU will write to the individual within one month of receiving the original request to tell them if this is the case.

v. If a subject access request is manifestly unfounded or excessive, RHSU is not obliged to comply with it. A subject access request is likely to be manifestly unfounded or excessive where it repeats a request to which the organisation has already responded. If an individual submits a request that is unfounded or excessive, the organisation will notify them that this is the case and whether or not it will respond to it

7.3 Other Rights

7.4 Individuals have a number of other rights in relation to their personal data. They can require the organisation to:

i. Rectify inaccurate data;
ii. Stop processing or erase data that is no longer necessary for the purposes of processing;
iii. Stop processing or erase data if the individual's interests override the organisation's legitimate grounds for processing data (where the organisation relies on its legitimate interests as a reason for processing data);
iv. Stop processing or erase data if processing is unlawful; and
v. Stop processing data for a period if data is inaccurate or if there is a dispute about whether or not the individual's interests override the organisation's legitimate grounds for processing data.

To ask the organisation to take any of these steps, the individual should send an email to helpdesk@su.rhul.ac.uk although all staff should understand how to recognise a request related to the above rights.

8. Data security

8.1 RHSU takes the security of personal data seriously. The organisation has the following controls in place to protect personal data against loss, accidental destruction, misuse or disclosure, and to ensure that data is not accessed, except by employees in the proper performance of their duties.

8.2 Training

8.3 Staff who process personal data will be provided with GDPR training as part of their induction process and at regular intervals thereafter.

8.4 Individuals whose roles require regular access to personal data, or who are responsible for implementing this policy or responding to subject access requests under this policy, will receive additional training to help them understand their duties and how to comply with them.

8.5 Impact assessments

8.6 Some of the processing that the organisation carries out may result in risks to privacy. Where processing would result in a high risk to individual's rights and freedoms, the organisation will carry out a data protection impact assessment to determine the necessity and proportionality of

processing. This will include considering the purposes for which the activity is carried out, the risks for individuals and the measures that can be put in place to mitigate those risks.

8.7 Third Party Processing

8.8 Where the organisation engages third parties to process personal data on its behalf, such parties do so on the basis of written instructions, are under a duty of confidentiality and are obliged to implement appropriate technical and organisational measures to ensure the security of data.

9. Data breaches

9.1 If the organisation discovers that there has been a breach of personal data that poses a risk to the rights and freedoms of individuals, it will report it to the ICO within 72 hours of discovery. The organisation will record all data breaches regardless of their effect.

9.2 If the breach is likely to result in a high risk to the rights and freedoms of individuals, it will tell affected individuals that there has been a breach and provide them with information about its likely consequences and the mitigation measures it has taken.

9.3 If you suspect a data breach has occurred or are made aware of a potential breach, please contact your line manager.

10. Monitoring and Reporting

10.1 The Board of Trustees will receive an annual report about the ongoing operation of this policy which will include:

i. Confirmation of the annual notification to ICO;
ii. A summary of related training and development activity across the Students' Union;
iii. A summary and analysis of any data breaches over the past year;
iv. The number of requests for access to personal data;
v. An analysis of any complaints from individuals or ICO.