Policy Title:	Data Protection Policy
Audience:	Staff and Members
Policy Date:	January 2017
Policy Revision Date:	May 2018 (new General Data Protection Regulations introduced)
Policy Locations:	N Drive: HR/AllUsers/Policies and Procedures PeopleHR / Company Documents

1. Introduction

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 1998 (DPA). This policy sets out how the organisation deals with personal data relating to staff, students, applicants and others.

2. Responsibilities

2.1. Royal Holloway Students' Union as an organisation is the 'Data Controller' as defined in the DPA and is ultimately responsible for the implementation of the Act. The primary contact to the Information Commissioner's Office (ICO) is the Chief Executive, who is responsible for maintaining the annual notification to ICO.

2.2. Heads of Departments 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 DPA principles outlined below.

2.3. Staff whose role requires them to process information about other people (including information connected with employment, study, student groups, or personal circumstances) must comply with this policy.

2.3.1. Staff who process or access personal data will be provided with Data Protection training as part of their induction and any refresher training as required by their line manager.

2.3.2. Staff who commission or employ third parties to process or handle personal data on behalf of, or in connection with, the Students' Union must ensure that the details of such processing are subject to a written agreement between the Students' Union and the third party. Third parties include suppliers or partners.

2.3.3. Further guidance for staff can be found in the associated Guidance to Data Protection for Employees.

3. Data protection principles

The DPA requires that eight data protection principles are followed in the handling of personal data. These principles require that personal data must:

i. be fairly and lawfully processed;
ii. be processed for limited purposes and not in any manner incompatible with those purposes;
iii. be adequate, relevant and not excessive;
iv. be accurate;
v. not be kept longer than is necessary;
vi. be processed in accordance with individuals' rights;
vii. be secure; and
viii. not be transferred to countries without adequate protection.

4. Personal data

The DPA applies only to information that constitutes 'personal data'. Information is 'personal data' if it:

i. identifies a person, whether by itself, or together with other information in the organisation's possession, or is likely to come into its possession; and
ii. is about a living person and affects that person's privacy (whether in their personal or family life, business or professional capacity) in the sense that the information has the person as its focus or is otherwise biographical in nature.

Consequently, automated and computerised personal information about employees and others held by organisations is covered by the Act. Personal information stored physically (for example, on paper) and held in any 'relevant filing system' is also covered. In addition,

information recorded with the intention that it will be stored in a relevant filing system or held on computer is covered.

4.1. The use of personal information

The DPA applies to personal information that is "processed". This includes obtaining personal information, retaining and using it, allowing it to be accessed, disclosing it and disposing of it.

4.2. Sensitive personal data

'Sensitive personal data' is information about an individual's:

i. racial or ethnic origin;
ii. political opinions;
iii. religious beliefs or other beliefs of a similar nature;
iv. trade union membership (within the meaning of the Trade Union and Labour Relations (Consolidation) Act 1992);
v. physical or mental health or condition;
vi. sex life;
vii. commission or alleged commission of any criminal offence; and
viii. proceedings for any offence committed or alleged to have been committed, the disposal of such proceedings or the sentence of any court in such proceedings.

The Students' Union will not retain sensitive personal data without the consent of the individual in question.

The organisation will process sensitive personal data, including sickness and injury records and references, in accordance with the eight data protection principles.

5. Employee data

An employee's personnel file is likely to contain information about their work history with the organisation and may, for example, include information about any disciplinary or grievance procedures, warnings, absence records, appraisal or performance information and personal information about the employee including address details and national insurance number.

There may also be other information about the employee located within the organisation, for example in their line manager's inbox or desktop; with payroll; or within documents stored in a relevant filing system.

The Students' Union may collect relevant sensitive personal information from employees for equal opportunities monitoring purposes. Where such information is collected, we will anonymise it, unless the purpose to which the information is put requires the full use of the individual's personal information. If the information is to be used, we will inform employees on any monitoring questionnaire of:

i. the use to which the data will be put
ii. the individuals or posts within the organisation who will have access to that information
iii. and the security measures that the organisation will put in place to ensure that there is no unauthorised access to it.

We will ensure that personal information about an employee, including information in personnel files, is securely retained. Any hard copies of information will be kept in a locked filing cabinet. Information stored electronically will be subject to access controls and passwords and encryption software will be used where necessary.

6. Membership Data and Data Sharing

6.1. The Students' Union is a separate, independent organisation to the College and as such both the College and RHSU are data controllers, as defined in the DPA, and will both process data in accordance with their respective notifications to the Information Commissioners Office and Data Protection policies. This means that each will be separately responsible for its own processing, and for ensuring that students' personal data is only processed for the purposes set out in their data processing statements or similar, or by subsequent agreement directly with the student.

6.2. Both organisations may on occasions work in partnership under the legitimate interests condition of the Act and, as such, agree to share the personal data of registered current students where necessary, and within the bounds of the DPA, to facilitate the administration of RHSU or to ensure individual students are appropriately supported during formal processes. This will not include the sharing of sensitive personal data.

6.3. College will provide RHSU with the following information as a minimum. Further requests for additional data may be considered in line with the principles above:

i. Student ID number
ii. Full name and title
iii. Date of birth
iv. Gender
v. College email address
vi. Personal email address (only for correspondence with confirmed applicants prior to arrival)
vii. Nationality
viii. Programme of study and mode, location and year of study
ix. Fee status

6.4. College will not share the personal data of students who have opted out of membership of RHSU at enrolment, except for student ID number and email address – to enable non-member access to services under the requirements of the Education Act 1994.

6.5. Personal data shared under this agreement will be kept secure and protected against unauthorised access, use or disclosure, and only retained for as long as necessary. If RHSU becomes aware of any potential data breach which involves data jointly owned by the College, the College Data Protection Officer must be alerted immediately. This includes any breach that occurs as a result of a direct action by a third party acting on the behalf of RHSU.

6.6. Should RHSU wish to contract out the processing of the shared data, it will ensure that the contract includes appropriate safeguards to ensure it discharges its responsibility as a Data Controller. In such an event the College Data Protection Officer is available to provide advice and support to RHSU.

6.7. The College will allow RHSU staff and those authorised to handle personal data access to their Data Protection training materials including the online module.

6.8. RHSU's Privacy Policy sets out how RHSU uses and protects membership information when using the website.

7. Data Subject Access Requests

An individual has the right to request to see a copy of the information the organisation keeps on them. Subject access provides a right for the requester to see their own personal data, rather than a right to see copies of documents that contain their personal data. Some types of personal data are exempt from the right of subject access and so cannot be obtained by making a SAR. Information may be exempt because of its nature or because of the effect its disclosure is likely to have. There are also some restrictions on disclosing information in response to a SAR – where this would involve disclosing information about another individual, for example.

Any Subject Access Request (SAR) should be made in writing to the Chief Executive. The Students' Union will make every effort to respond to any such request promptly, and in any event within 40 calendar days of receiving it. The organisation will charge £10 for allowing individual's access to information about them, which is a contribution towards the administration cost.

8. Monitoring and Reporting

The Board of Trustees will receive an annual report about the ongoing operation of this policy which must 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 all requests for access to personal data
- **v.** an analysis of any complaints from individuals or ICO.