Royal Agricultural University

Data Protection Policy

Policy Ref (to be assigned by IPG): IPG001	VCAG Policy Owner (policy updater): Graham Pollard, Chief Operating Officer
Approving Body: VCAG	VCEG Lead: Matt Jones, Director of Institutional Planning & Policy
Date Approved:	Review Date:

Introduction

1.1 The Royal Agricultural University (RAU) collects, holds and processes data about its students, employees, applicants, alumni, stakeholders, contractors and other individuals in order to carry out its business and organisational functions.

1.2 Data protection legislation defines 'personal data' as any information relating to an identified, or an identifiable natural person ('data subject'). An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. Personal data also includes any expression of opinion about the data subject and what is intended for them.

1.3 The University is committed to protecting the rights and freedoms of individuals with respect to the processing of their personal data.

Policy Statement

2.1 The University is committed to complying with Data Protection legislation through its everyday working practices.

2.2 Complying with Data Protection legislation may be summarised as, but is not limited to:

- understanding, and applying as necessary, the data protection principles when processing personal data;
- understanding, and fulfilling when necessary, the rights given to data subjects under Data Protection legislation;
- understanding, and implementing as necessary, the University's accountability obligations under Data Protection legislation.

2.3 In accordance with Data Protection legislation, additional conditions and safeguards will be applied to ensure that special category data (sensitive personal data) is handled appropriately. Special category personal data is information relating to an individual's:

- race or ethnic origin;
- political opinions;
- religious beliefs or other beliefs of a similar nature;
- trade union membership;

- genetic data;
- biometric data (where used for identification purposes);
- health;
- sex life or sexual orientation.

2.4 Criminal convictions or offences (alleged or proven) are not technically defined as special category personal data but are afforded similar protections.

Data Protection Principles

3.1 Data Protection legislation requires that the University, its staff and others who process or use any personal information, comply with the data protection principles.

3.2 The data protection principles state that personal data should be:

- processed lawfully, fairly and in a transparent manner;
- collected for specified, explicit and legitimate purposes;
- adequate, relevant and limited to what is necessary;
- accurate and where necessary kept up to date;
- kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which that data is processed;
- processed in a manner that ensures appropriate security of the personal data.

3.3 Accountability is central to Data Protection legislation, and Data Controllers are responsible for compliance with the principles and must be able to demonstrate this to data subjects and the UK regulator, the ICO.

Data Subject Rights

4.1 The rights given to data subjects under Data Protection legislation are:

- the right to be informed;
- the right of access to the information held about them (through a Subject Access Request);
- the right to rectification;
- the right to erasure;
- the right to restrict processing;
- the right to data portability;
- the right to object;
- rights in relation to automated decision-making and profiling.

4.2 Under Data Protection Regulation legislation, data subjects have the right of access to their personal data held by the University.

4.3 Any individual who wishes to exercise this right should make the request in one of the following ways:

- Write directly to the FOI secretary, Royal Agricultural University, Cirencester, GL7 6JS, stating name, address and details of the information that is required.
- Email foi@rau.ac.uk stating name, address and details of the information that is required.

4.4 When the request is received, a search should be instigated for the information needed. If it cannot be determined exactly what information is required, contact should be made as soon as possible to clarify the request. If the information requested is already published, details will be sent on how to find the information.

4.5 If the information is exempt from the requesters access, the RAU must provide the information that they are able to and also provide reasons why the other information cannot be released.

4.6 The RAU reserves the right to charge a fee to cover the costs of the search and any copying.

Scope

3.1 This policy applies to all personal data we process regardless of the location where that personal data is stored (e.g. on an employee's own device) and regardless of the data subject. All staff and others processing personal data on the University's behalf must read it. A failure to comply with this policy may result in disciplinary action.

3.2 All Deans of Schools and Directors of Professional Services are responsible for ensuring that all University staff within their area of responsibility comply with this policy and should implement appropriate practices, processes, controls and training to ensure compliance.

3.3 The Institutional Planning & Governance Directorate (IPG) are responsible for overseeing this policy.

3.4 The University's Data Protection Officer (DPO) is Matt Jones, Director of Institutional Planning and Policy and can be reached at data.protection@rau.ac.uk.

Relevant legislation / guidance

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

Freedom of Information Act 2000

Data Breach Policy

Data Protection Handbook

Data Incident Reporting Form

Further guidance can be found on the Information Commissioner's Officer (ICO) website – https://ico.org.uk/

Policy details

4 Definitions

4.1 Personal Data means any information relating to an identified or identifiable natural living person (**'data subject'**); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

4.2 Processing means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means.

4.3 Data controller means any individual or organisation which either alone or jointly, determines the purposes and means of the processing of personal data.

4.4 Data processor means any individual or organisation which processes personal data on behalf of a controller.

4.5 Personal data breach means a breach of security or process leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

5 Personal data protection principles

5.1 When you process personal data, you should be guided by the following principles, which are set out in the GDPR. The University is responsible for, and must be able to demonstrate compliance with, the data protection principles listed below:

5.2 Those principles require personal data to be:

- processed lawfully, fairly and in a transparent manner (**lawfulness, fairness and transparency**).
- collected only for specified, explicit and legitimate purposes and not further processed in a manner incompatible with those purposes (purpose limitation).
- adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed (**data minimisation**).
- accurate and where necessary kept up to date (**accuracy**).
- not kept in a form which permits identification of data subjects for longer than is necessary for the purposes for which the personal data is processed (**storage limitation**)
- processed in a manner that ensures its security, using appropriate technical and organisational measures to protect against unauthorised or unlawful processing and against accidental loss, destruction or damage (**security, integrity and confidentiality**).

6 Policy guidelines

6.1 The University will comply with the principles of the UK General Data Protection Regulations when processing any personal data.

6.2 The University will only process personal data where it can match processing activities to one or more of the lawful bases for processing under Article 6(1) of the UK GDPR or in the case of special category personal data Article 9(1) of the UK GDPR.

6.3 The University will ensure that a record of the processing activity it undertakes is maintained (as required by the UK GDPR) and made available to the relevant authority (the ICO in the UK), upon request.

6.4 The University will ensure that all new and significantly amended systems are subject to sufficient Data Privacy Impact Assessment (DPIA), and the risks identified are appropriately managed. For internal processes or systems this will be in the form of a Privacy Impact Assessment (PIA) and where there is the involvement of an external partner (data processor) who will handle or store information on behalf of the University, a Supplier

Information Security Assessment (SISA) will be used to assess their technical security arrangements.

- By default, the minimum of information classification (please see information classification process) which will be used for records containing personal data will be restricted, and for those records containing special category data confidential, and the controls outlined in the information classification will be followed.
- The University will ensure that all requests made by data subjects in accordance with the UK GDPR are handled appropriately and within the prescribed time limits (30 calendar days, from receipt of sufficient evidence of identity, for Subject Access Requests). Where requested to do so, the University will also advise the data subject of the purposes for which the data is to be processed and the recipient or classes of recipients to which the data are or may be disclosed (please see guidance document).
- In the event of a personal data breach the University will use a managed, documented approach to managing the incident, the University will use a managed, documented approach to managing the incident including assessing the severity of the incident, and where applicable will notify the ICO within 72 hours of becoming aware of the incident (please see guidance document).

Training and Education

- All staff and contractors of the Royal Agricultural University and its subsidiary companies who do or are likely to come into contact with personal data in carrying out their responsibilities are required to receive Data Protection Training, on this basis the University will:
  - ensure that all new staff and contractors of the University receive appropriate Cyber Security and GDPR training as part of their induction, and that, until such training has been undertaken, access to systems and storage media containing personal information will be prohibited.
  - Ensure that all existing staff and contractors of the University undertake appropriate Cyber Security and GDPR training, which will be refreshed on a two-yearly basis. Staff who fail to undertake this training will have their IT account suspended, and thus their access to personal information will be revoked until training is complete.
- This policy will come into effect on the *(Date).*
- This policy will be uploaded to our website and staff intranet, along with all associated processes, procedures and guidance notes.
- Training will be available for those members of staff who do not have access to a computer and subsequent policies and materials provided.

Responsibilities

Everyone who works for or with the Royal Agricultural University has some responsibility for ensuring data is collected, stored and handled appropriately. Each team that handles personal data must ensure that it is handled and processed in line with this policy and UK GDPR principles. It is important to note that a breach in this policy could lead to disciplinary proceedings and a significant fine for the RAU.

The Board of Governors is ultimately responsible for ensuring that the RAU meets its legal obligations.

The Data Protection Officer is responsible for:

- Informing and advising the organisation and its employees of their data protection obligations under the UK GDPR.
- Monitoring the organisation's compliance with the UK GDPR and internal data protection policies and procedures. This will include monitoring the assignment of responsibilities, awareness training, and training staff involved in processing operations and related audits.
- Advising on the necessity of data protection impact assessments (DPIAs), the manner of their implementation and their outcomes.
- Serving as the contact point to the data protection authorities for all data protection issues, including data breach reporting.
- Serving as the contact point for individuals (data subjects) on privacy matters, including subject access requests.

The Director of Digital Innovation is responsible for:

- Developing technical security standards to be used across the Royal Agricultural University.
- Ensuring teams across the University carry out regular checks and scans to ensure security hardware and software is functioning properly.
- Evaluating the technical security arrangements of any third-party services the RAU is considering using to store or process data, using a Supplier Information Security Assessment to gather evidence. *Appendix 3.*

Equality, Diversity and Inclusion

The University collects and analyses staff and student data across the protected characteristics to help us assess the impact of our policies and practices on equality and good relations. This is important for:

- identifying inequalities;
- setting objectives and targets;
- prioritising activity;
- planning engagement;
- minimising negative impact; and
- enhancing positive impact.

Information on why this data is collected and how it is used, can be found in our Equality, Diversity and Inclusion Strategy 2021-2025. and our Access and Participation Plan (APP) 2021-2025. All personal data collected for these purposes, will be protected under this policy.

Other related policies / procedures

Data Protection Handbook to support the Royal Agricultural University Data Protection Policy.

Consequences

A breach in this policy could lead to disciplinary proceedings and a significant fine for the RAU.

Review

This policy will be reviewed every year.

Version control

Version number	Change	Name and job title	Date
001	Whole policy update	Sara Papps – Head of Planning, Data & Business Intelligence	19th October 2023