Royal Agricultural University

Policy and Procedures Relating To
Data Protection

1. Overview

The purpose of this policy is to ensure that the Royal Agricultural University's staff and students comply with the provisions of the Data Protection Act 1998 and the General Data Protection Regulation when processing personal data. Any infringement of the Act or the Regulation will be treated seriously by the University and may be considered under disciplinary procedures.

The University needs to collect and use data for a number of purposes about its staff, students and other individuals who come into contact with the University. In collecting and using this data, the University is committed to protecting an individual's right to privacy with regard to the processing of personal data and this policy has been implemented to support this commitment.

This policy sets out the rules that all RAU staff, students, and contractors, who process or use any personal information on behalf of the University are subject to in order to ensure that the University is compliant with its obligations under the Act.

The Act and the Regulation govern the collection, holding, processing and retention of all personal data relating to living individuals. Its purpose being to ensure that those organisations and individuals, who collect, store and use that data do not abuse it, and process the data in accordance with the following eight Data Protection Principles that personal data shall be:

- Processed fairly and lawfully.
- Obtained only for one or more specified and lawful purpose.
- Adequate, relevant and not excessive for those purposes.
- Accurate and kept up to date - data subjects have the right to have inaccurate personal data corrected or destroyed if the personal information is inaccurate to any matter of fact.
- Kept for no longer than is necessary for the purposes it is being processed.
- Processed in line with the rights of individuals - this includes the right to be informed of all the information held about them, to prevent processing of their personal information for marketing purposes, and to compensation if they can prove they have been damaged by a data controller's non-compliance with the Act.
- Secured against accidental loss, destruction or damage and against unauthorised or unlawful processing - this applies to you even if your business uses a third party to process personal information on your behalf.
- Not transferred to countries outside the European Economic Area - unless that country has equivalent levels of protection for personal data.

The University and its staff, students, contractors, and partnership organisations that process or use personal data on behalf of the University must comply with these principles and ensure that they are followed at all times. As stated, the Act covers all personal data that is held electronically, including databases, email and the Internet / Intranet, as well as paper records. It also includes photographs, audio recordings and CCTV or webcam footage. The paper records that are subject to the Act and the Regulation are those that are contained in a ‘relevant filing system’ where the data is organised and structured.

2. Responsibilities

It is the responsibility of the Senior Management of the RAU to ensure that staff have received appropriate training in data protection.

It is the responsibility of every member of staff to act in accordance with the policy and any training provided.

3. Individual Consent

The University primarily processes staff and student data on the basis of contract or legitimate interest. It is a condition of student enrolment and of staff employment that they agree to the University processing necessary personal information as part of the University’s statutory legal obligations.

The University may process some information that is categorised as ‘special category data’; this includes information about an individual’s racial or ethnic origin, gender, religion and beliefs, genetics or biometrics, sexual orientation, physical or mental health, and criminal convictions, charges or proceedings. Processing this information is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law.

Direct Marketing

An individual has the right to prevent his/her personal data being processed for direct marketing. An individual can, at any time, give written notice to stop (or not begin) using their personal data for direct marketing. The policy of the RAU is to comply with all such requests by an individual.

4. Data Processing

As and when staff, students, and contractors are required to collect personal data they must adhere to the requirements of this policy and any applicable local guidelines. Students may process personal data in connection with their studies. If they do they should be advised to inform their tutor, who will make any necessary enquiries with the Data Protection Officer.

5. Information Disclosure

The University requires all staff, students, and contractors to be vigilant and exercise caution when asked to provide personal data held on another individual. In particular, they must ensure that personal information is not disclosed either orally or in writing to any unauthorised personnel, which includes family members, friends, government bodies and in certain circumstances the police, without the express prior consent of the relevant individual.

6. Data Security

All staff, students, contractors, and partnership organisations must ensure that any personal information which they hold is kept securely and that they take appropriate security precautions by seeking to ensure the following:

- Source documents kept in a lockable cabinet or drawer or room;
- Computerised data is password protected;
- Data kept on discs or data storage devices are stored securely and password protected or encrypted;

- Individual passwords are kept confidential and are not disclosed to other personnel enabling log-in under another individual's personal username and password;
- Logged on PCs are not left unattended where data is visible on screen to unauthorised personnel and that screensavers are used at all times;
- Paper-based records are never left where unauthorised personnel can read or gain access to them.

When manual records are no longer required, they should be shredded or bagged and disposed of securely, and the hard drives of redundant PCs should be wiped clean.

Off-site use of personal data presents a greater risk of loss, theft or damage and the institutional and personal liability that may accrue from the off-site use of personal data is similarly increased. For these reasons staff and others should:

- only take personal data off-site when absolutely necessary and for the shortest possible time;
- take particular care when laptops or personal machines are used to process personal data at home or in locations outside of the University, they are kept secure at all times. No Personal Data is to be downloaded to the C drive on University computers, or to your personal machine.

7. Access to Personal Data

Subject to exemptions, the Act and the Regulation give any individual who has personal data kept about them at the University the right to request in writing a copy of the information held relating to the individual.

Any member of staff who wants to exercise this right should in the first instance make a written request to the HR department. External requests are made via the Data Protection Officer.

The University aims to comply with requests for access to personal information as quickly as possible, but will endeavour to provide the data within the 30 day limit set down by the General Data Protection Regulation, unless there are extenuating circumstances in which case the 90 day rule may apply.

The Regulation does not prevent an individual making a subject access request via a third party, including by a solicitor acting on behalf of a client. In these cases and prior to the disclosure of any personal information, the University would need to be satisfied that the third party making the request is entitled to act on behalf of the individual and would require evidence of this entitlement.

8. Accuracy of Data

Staff are responsible for:

- ensuring that any information they provide to the University relating to their employment is accurate and up to date;
- informing the University of any information changes, eg. change of address; and
- checking the information that the University may send out from time to time giving details of information kept and processed about staff.

Students must also ensure that all data provided to the University is accurate and up-to-date by either notifying their Centre Secretary or the Registrar.

The University cannot be held responsible for any errors unless the student has informed the University about changes to their circumstances.

11. Retention and Disposal of Data

The University is not permitted to keep personal information of either students or staff for longer than is required for its purpose. However, some data will be kept longer or in perpetuity to comply with statutory or funding body requirements.

Personal and confidential information will be disposed of by means that protect the rights of those individuals ie. shredding, disposal of confidential waste, secure electronic deletion.

12. Complaints

The University is dedicated to being compliant with the Act and the Regulation. Individuals, any member of staff or a student wishing to report concerns should contact the Data Protection Officer. The complaint will be acknowledged immediately and every reasonable effort will be made to offer a more comprehensive reply within 21 days.

13. Portability

The University recognizes the right of individuals to have their personal data to be moved, copied or transferred to another IT environment in a safe and secure way, without hindrance to usability.

14. Compliance Monitoring

To confirm that an adequate level of compliance is being achieved by all departments of the RAU, the Data Protection Officer ("DPO") may instigate from time to time Data Protection Audits.

Each Audit will assess:-

1. Compliance with Policy in relation to the protection of Personal Data
2. The effectiveness of Data Protection in relation to operational practices
3. The level of understanding of Data Protection Policies and Privacy Notices
4. The Accuracy of Personal Data being stored
5. The conformity of Personal Data Processing activities
6. The Adequacy of Procedures for redressing poor Compliance and Personal Data Breaches.

15. Training

All members of staff that have access to Personal Data must complete to a satisfactory standard the Data Protection (GDPR) Training.

RAU Staff Privacy Policy			
Version	Drafted by	Date	Approved
1.1	Hannah Langford (GDPR Project Lead)	20.04.18	20.05.18