Data Breach Policy

Policy Ref (to be assigned by IPG): IPG002	VCAG Policy Owner (policy updater): Chief Operating Officer
Approving Body: VCAG	VCEG Lead: Director of Institutional Planning & Policy
Date Approved: December 2023	Review Date: December 2025

Introduction

1.1 The Royal Agricultural University collects, holds, processes, and shares personal data, a valuable asset that needs to be suitably protected.

1.2 Every care is taken to protect personal data from incidents (either accidentally or deliberately) to avoid a data protection breach that could compromise security.

1.3 Compromise of information, confidentiality, integrity, or availability may result in harm to individual(s), reputational damage, detrimental effect on service provision, legislative noncompliance, and/or financial costs.

Policy Statement

2.1 The aim of this policy is to promote and standardise the University wide approach and response to any data breach incident, to ensure incidents are reported, logged and managed appropriately by adopting a standard consistent approach to all data security incidents, it aims to ensure that;

- Incidents are reported in a timely manner and can be properly investigated.
- Incidents can be managed by relevant stakeholders, skilled and authorised personnel, and consideration given to the referral to the Information Commissioners Office/supervisory authority where appropriate to do so ensuring the 72-hours statutory period is met.
- All incidents are recorded and documented, evidence gathered and maintained in a form that will withstand internal and external security.
- The notification of any data subjects and or external bodies where appropriate.
- The impact of incidents and actions taken to prevent reoccurrence and identify improvements in policies and procedures.

Scope

3.1 This University policies applies to all personal data processed by the University, regardless of format and is applicable to all staff, students, visitors, contractors and data processors acting on behalf of the University.

Relevant legislation / guidance

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

Data Protection Policy.

Data Protection Handbook.

Data Incident Reporting Form.

Policy details

4 Definitions

4.1 For the purpose of this policy, data security breaches include both confirmed and suspected incidents.

4.2 An incident in the context of this policy is an event or action which may compromise the confidentiality, integrity or availability of systems or data, either accidentally or deliberately, and has caused or has the potential to cause damage to the University's information assets and/or reputation.

4.3 An incident includes but is not restricted to, the following:

- Loss or theft of confidential or sensitive data or equipment on which such data is stored (e.g. loss of laptop, USB stick, iPad/tablet device, or paper record);
- Equipment theft or failure;
- System failure;
- Unauthorised use of, access to or modification of data or information systems;
- Attempts (failed or successful) to gain unauthorised access to information or IT system(s);
- Unauthorised disclosure of sensitive/confidential data;
- Website defacement;
- Hacking attack;
- Unforeseen circumstances such as a fire or flood;
- Human error;
- 'Blagging' offences where information is obtained by deceiving the organisation who holds it.

5 Reporting an incident

5.1 Any individual who accesses, uses or manages the University's information is responsible for reporting data breach and information security incidents immediately to the Data Protection Officer data.protection@rau.ac.uk.

5.2 If the breach occurs or is discovered outside normal working hours, it must be reported as soon as it practicable.

5.3 You will be asked to complete a Data Incident Report Form, which can be found here. The form must include full and accurate details of the incident, when the occurred (dates and times), who is reporting it, if the data relates to people, the nature of the information, and how many individuals are involved.

5.4 All staff should be aware that any breach of Data Protection legislation may result in the University's Disciplinary Procedures being instigated.

6 Containment and Recovery

6.1 The Data Protection Officer (DPO) will firstly determine if the breach is still occurring. If so, the appropriate steps will be taken immediately to minimise the effect of the breach.

6.2 An initial assessment will be made by the DPO in liaison with relevant staff to establish the severity of the breach and who will take the lead investigating the breach.

6.3 The DPO will establish whether there is anything that can be done to recover any losses and limit the damage the breach could cause.

6.4 The DPO will establish who may need to be notified as part of the initial containment and contact any relevant authorities, if necessary.

6.5 Advice from experts across the University may be sought in resolving the incident promptly.

6.6 The DPO will determine the suitable course of action to be taken to ensure a resolution to the incident.

7 Investigation and Risk Assessment

7.1 An investigation will be undertaken by the DPO immediately and wherever possible, within 24 hours of the breach being discovered/reported.

7.2 The DPO will investigate the breach and assess the risks associated with it, for example, the potential adverse consequences for individuals, how serious or substantial those are and how likely they are to occur.

7.3 The investigation will need to consider the following:

- the type of data involved;
- its sensitivity;
- the protections that are in place (e.g. encryptions);
- what has happened to the data (e.g. has it been lost or stolen);
- whether the data could be put to any illegal or inappropriate use;
- data subject(s) affected by the breach, number of individuals involved and the potential effects on those data subject(s);
- whether there are wider consequences to the breach.

8 Notification

8.1 The DPO, in consultation with relevant colleagues will establish whether the Information Commissioner's Office will need to be notified of the breach, and if so, notify them within 72 hours of becoming aware of the breach, where feasible.

8.2 Every incident will be assessed on a case by case basis; however, the following will need to be considered:

- whether the breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms under Data Protection Legislation;
- whether notification would assist the individual(s) affected (e.g. could they act on the information to mitigate risks?);
- whether notification would help prevent the unauthorised or unlawful use of personal data;
- whether there are any legal/contractual notification requirements;
- the dangers of over notifying. Not every incident warrants notification and over notification may cause disproportionate enquiries and work.

8.3 Individuals whose personal data has been affected by the incident, and where it has been considered likely to result in a high risk of adversely affecting that individual's rights and freedoms, will be informed without undue delay. Notification will include a description of how and when the breach occurred and the data involved. Specific and clear advice will be given on what they can do to protect themselves, and include what action has already been taken to mitigate the risks. Individuals will also be provided with a way in which they can contact the University for further information or to ask questions on what has occurred.

8.4 The DPO must consider notifying third parties such as the police, insurers, banks or credit card companies, and trade unions. This would be appropriate where illegal activity is known or is believed to have occurred, or where there is a risk that illegal activity might occur in the future.

8.5 The DPO will consider whether the communications manager should be informed regarding a press release and to be ready to handle any incoming press enquiries.

8.6 A record will be kept of any personal data breach, regardless of whether notification was required.

9 Evaluation and Response

9.1 Once the initial incident is contained, the DPO will carry out a full review of the causes of the breach; the effectiveness of the response(s) and whether any changes to systems, policies and procedures should be undertaken.

9.2 Existing controls will be reviewed to determine their adequacy, and whether any corrective action should be taken to minimise the risk of similar incidents occurring.

9.3 The review will consider:

- where and how personal data is held and where and how it is stored;
- where the biggest risks lie including identifying potential weak points within existing security measures;
- whether methods of transmission are secure; sharing minimum amount of data necessary;
- staff awareness;
- implementing a data breach plan and identifying a group of individuals responsible for reacting to reported breaches of security.

9.4 If deemed necessary, a report recommending any changes to systems, policies and procedures will be considered by the Vice Chancellors Executive Committee (VCEG).

Responsibilities

10.1 Everyone who works for or with the Royal Agricultural University has some responsibility for ensuring data is collected, stored and handled appropriately, in the instance of a Data Breach, the following are responsible for each area:

- **VCEG** has overall responsibility to ensure that the University meets its legal and regulatory obligations.
- The **Data Protection Officer (DPO)** has responsibility to brief and escalate data breaches where necessary to the **VC** and **Governing Body**. The DPO will determine the necessity to report to the Information Commissioners Office and make recommendations.
- **Directorate Leads/Faculty Leads** are responsible for ensuring that staff in their area act in compliance with the policy and provide appropriate assistance to investigations as required.
- **Information Users** – All staff, contractors will be aware of their responsibilities and reporting procedures where there is a personal data breach whether actual, suspected or potential should:
  - Inform line manager immediately;
  - Take steps to retrieve/contain the personal data;
  - Notify the DPO as soon as possible by completing the Data Incident Report Form
  - Assist with investigations as required and particularly if urgent action must be taken to prevent any further damage.
- All staff should be aware that any breach of Data Protection legislation may be subject to the University's disciplinary procedures.

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

All staff should be aware that any breach of Data Protection legislation may be subject to the University's disciplinary procedures.

Review

This policy will be updated as necessary to reflect best practice and to ensure compliance with any changes or amendments to relevant legislation, but will be routinely reviewed every two years.

Version control

Version number	Change	Name and job title	Date
001	Whole policy update	Sara Papps – Head of Planning, Data & Business Intelligence	31st October 2023