Data Breach Policy

1. Introduction

1.1 The University of Kent collects, processes and retains data in order to deliver its operational and strategic objectives and to support its business functions.

1.2 When processing personal data, the University has a legal obligation to ensure that it complies with the requirements made in the United Kingdom General Data Protection Regulation (UK GDPR), the Data Protection Act 2018 (DPA 2018) and any other related legislation, including the EU GDPR if applicable.

1.3 As part of those obligations, the University must ensure the processing of appropriate safeguards.

1.4 If these safeguards fail, the University has a legal duty to maintain processes for the detection, reporting and management of incidents involving the breach of personal data.

2. Definitions

2.1 For the purposes of this policy, 'personal data' is defined as information relating to natural persons who:

- can be identified or who are identifiable, directly from the information in question or
- can be indirectly identified from that information in combination with other information.

2.2 This policy applies to personal data for which the University is the registered data controller and is also applicable when an external party is processing such data.

2.3 'Data breach' is defined as an incident where there has been a breach of security around personal data which has in turn lead to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

3. Purpose of this policy

3.1 This policy details how the University of Kent intends to meet its legal obligations around the reporting and management of personal data breaches, by:

- detailing the procedure by which staff must report personal data breaches to the designated Data Protection Officer (DPO)
- confirming the duty of staff to assist the Data Protection Officer and their staff in respect to the handling of personal data breaches
- outlining the factors which must be considered when risk assessing the impact and severity of a personal data breach and
- establishing the institutional framework within which data breaches must be managed and recorded, in order to reduce the impact, severity and risk associated with data breaches.

4. Reporting a personal data breach

4.1 On becoming aware of a potential breach of personal data, staff must immediately report the breach to the Assurance and Data Protection Office.

4.2 When reporting a breach, staff shall be required to provide the following information to the Assurance and Data Protection Office:

- a description of the personal data affected
- an explanation of the incident, how it happened and when
- the types and approximate number of data subjects concerned
- the categories and approximate number of personal data records concerned
- the likely consequences of the personal data breach
- any immediate attempts to reduce the impact of the breach.

4.3 Staff will be asked to complete the Data Incident Evaluation Report Form attached at Appendix A. Lack of clarity around the circumstances surrounding the potential breach must not delay the reporting of breaches to the Assurance and Data Protection Office.

4.4 Staff must assist the Assurance and Data Protection Office in the management of the breach and must respond in a timely manner to any queries raised by the Assurance and Data Protection Office during any associated investigations.

4.5 The University may appoint external processors to process data on its behalf. Any associated contract must require the processor to inform without delay the University's Data Protection Officer of any potential personal data breach affecting University controlled data.

4.6 If a staff member becomes aware that a processor or sub-processor has experienced a personal data breach, they must inform the Assurance and Data Protection Office as they would any other breach.

4.7 The Data Protection Officer must take reasonable steps to ensure that all staff are aware of the reporting mechanism contained in this section.

5. Breach management

5.1 On receipt by the Assurance and Data Protection Office, the Data Protection Officer will assess whether the potential breach is likely to result in a material risk to the rights and freedoms of the data subjects concerned.

5.2 If the Data Protection Officer considers the potential breach would result in a severe/high risk to the rights and freedoms of the data subject, they shall report the breach as soon as is practicable to the Information Commissioner's Office, and by the latest within 72 hours of University of Kent becoming aware of the breach.

5.3 Where a breach or potential breach is not deemed to be reportable, the Assurance and Data Protection Office shall define the breach or potential breach as a 'Data security incident' or 'Non-reportable data breach'.

5.4 When assessing the risk posed by the breach to data subjects, the Data Protection Officer shall consider the following factors:

- the type of breach
- the nature, sensitivity and volume of personal data
- ease of identification of individuals
- severity of consequences to individuals
- special characteristics of the individuals affected
- the number of affected individuals

5.5 Where there is a lack of detail around the causes and potential impact of a breach, the Data Protection Officer should include that as a factor when assessing the overall risk.

5.6 Where there has been a serious breach (and the Data Protection Officer has identified a high risk to data subjects) the Assurance and Data Protection Office will contact the data subjects concerned, without undue delay and informing them of, as a minimum:

- a description of the nature of the breach
- the name and contact details of the Data Protection Officer and/or other relevant contacts

- a description of the likely consequences of the breach and
- a description of the measures taken or proposed to be taken by the controller to address the breach, including, where appropriate, measures to mitigate its possible adverse effects.

5.7 The Data Protection Officer will inform the Secretary to the University Council of any reportable breaches, who will in turn keep the Executive Group informed of the situation as it progresses.

5.8 All breaches will be investigated by the Data Protection Officer through the Assurance and Data Protection Office.

5.9 The Data Protection Officer will advise and assist the reporting department to take steps to contain any potential breach, mitigate any resulting risks and put in place remedies so as to reduce the impact of any potential breaches on the data subject concerned.

5.10 If during the course of their investigations, the Assurance and Data Protection Office uncovers further information that changes the nature of a minor data breach so that the breach becomes reportable, the Data Protection Officer must inform the Information Commissioner's Office of the breach without delay.

5.11 Where, on further investigation, it is apparent that the breach did not disclose personal data, the Assurance and Data Protection Office will deem the incident as a 'data security incident'.

5.12 The University of Kent in collaboration with the Data Protection Officer will assist the Information Commissioner's Office in the exercise of its statutory powers concerning reportable data breaches and will consider any advice given by the Information Commissioner's Office around the management of a reported data breach.

5.13 The Assurance and Data Protection Office will maintain a log of all breaches, reportable as well as minor, as well as a record of all actions and decisions made by the Data Protection Officer in respect of the management of that breach.

5.14 The Assurance and Data Protection Office shall also record data security incidents in order to identify potential non-compliance with established policy.

6. Personal data breaches resulting from cyber security incidents

6.1 In circumstances where the security of personal data has been compromised by a cyber-incident, the Data Protection Officer shall ensure that the breach is managed according to the requirements made in this policy, in conjunction with those detailed in the Information Security Major Incident Plan.

7. Evaluation and 'lessons learnt'

7.1 Once the personal data breach has been contained and remedial actions completed, the Data Protection Officer shall review the causes of the personal data beach and the University's response to the breach.

7.2 The Data Protection Officer's evaluation will be communicated to the senior management of the operational area in which the breach occurred.

7.3 The evaluation will also be communicated to the University's Information Custodian's Network to ensure a 'lessons learnt' approach is embedded in the data breach process.

7.4 The Data Protection Officer will include relevant statistics and summaries around data breaches in their regular reports to the Executive Group of the University of Kent.

Document review date

This policy will be reviewed annually by the Data Protection Officer

Version	Author	Description of Change	Date	Next Review date
0.1	Head of Data Protection	Policy created	2 March 2020	2 March 2021
0.2	Assurance Team	Updated to reflect change in the law since 01.01.21 update new team name and minor stylistic amendments. 4.2 'affected' 'an explanation of the incident, how it happened and when' and' likely consequences of the breach added. 4.3 Appendix A: Data incident evaluation form added. 5.2 addition of 'a severe/high' and 'rights and freedoms of' 5.3, 5.11,5.14 Updated to reflect new form terminology. 5.8 'both minor and reportable' deleted. 5.9 'advise and assist the reporting team' added.	12 April 2022	12 April 2023
0.2	Audit Committee	Recommendation to change 'should' to 'must' in paragraphs 3, 4.3 and 4.4	14 June 2022	

Document approval

Version	Governing Body	Approval Date
0.1	EG	02 March 2020
0.2	EG	06 June 2022
0.2	Audit Committee	14 June 2022

Appendix A: Data incident evaluation form

Data incident evaluation report template

To be completed as far as possible by the individual reporting the data incident.

Note: If it is possible to retrieve the information retrieve it as soon as possible e.g., recalling e-mails.

In order to evaluate the data security incident, it is necessary to define:

1 Initial information gathering:

- what has happened;
- when and how you found out about the breach;
- the people that have been or may be affected by the breach;
- what you are doing as a result of the breach; and
- who else you have told.

To ensure that the evaluation is appropriate and to help the Assurance and Data Protection Office provide the most effective support to you. Please provide as much information as possible and ensure it is as accurate and detailed as possible.

For completion by Assurance and Data Protection Office:

a. Follow up/interim
b. Conclusion/Lessons Learned, Article 33(5) record

****

Contact(s):

Department:

DPO: Laura Pullin

Type of Data:

Other e.g., software provider:

2. Incident Details

Date & Time of Incident:

What happened? Please provide as much information as possible:

How was the incident discovered?

How many data subjects are affected by the breach?

Category and number of people information disclosed to:

Total number of people:

Number of staff?

Number of students?

Number of visitors?

Number of others?

Is the incident likely to result in:

- ☐ **A high risk (to subject)**
- ☐ **Moderate**
- ☐ **Low**
- ☐ **None - see mitigation**

Information Disclosed relates to:

- ☐ Name
- ☐ Address
- ☐ Phone Number
- ☐ Email
- ☐ Bank Details

☐ Other

Was Special Category data disclosed?:

☐ No

☐ Personal data revealing racial or ethnic origin

☐ Personal data revealing political opinions

☐ Personal data revealing religious or philosophical beliefs

☐ Personal data revealing trade union membership

☐ Genetic data

☐ Biometric data (where used for identification purposes)

☐ Data concerning health

☐ Data concerning a person's sex life

☐ Data concerning a person's sexual orientation

Was this a Cyber Incident?:

☐ Yes

☐ No

3. Mitigation

What steps have been taken to mitigate the impact of this incident? (E.g., attempt to retrieve/contain information)

Has data protection training been completed by the staff member(s) involved in this incident?

☐ Yes

☐ No

If Yes, what training has been completed and when?

If no data protection training has been completed, please explain why?

4. *Investigation and Evaluation (for completion by Assurance & Data Protection Office)*

Other Mitigation:

Lessons Learned:

Conclusion (Reportable Data Breach / Non-Reportable Data Breach / Data Security Incident)

The Data Protection Officer will use the information provided on this form to assess the incident and conclude whether it is a: Reportable data breach, non-reportable data breach, or non-reportable data security incident.