UNIVERSITY OF HULL

Data Breach Policy

Classification:	**Policy**
Version Number:	0-04
Status:	Approved
Approved by:	IGC, University Secretary
Approval Date:	04/08/2022
Effective from:	04/08/2022
Next Review Date:	04/08/2024
Document Author:	Angela Clement, Data Protection Officer
Document Owner:	Governance & Compliance
Department/Contact:	dataprotection@hull.ac.uk
Collaborative provision:	Please state whether this document is applicable to the university's collaborative partners: ☒ Mandatory ☐ Not mandatory
Related documents:	Data Protection Policy, Data Classification Policy, Information Systems Security & Architecture Policy
Published location:	Internally

All printed or downloaded versions of this document are classified as uncontrolled.
A controlled version is available from the university website.

This document is available in alternative formats from
policy@hull.ac.uk

UNIVERSITY OF HULL

Data Breach Policy

Table of Contents

UNIVERSITY OF HULL

UNIVERSITY OF HULL

Data Breach Policy

1. Introduction

1.1 The University of Hull (the 'University') collects, holds, processes and retains personal data to deliver and support its business function.

1.2 Under the General Data Protection Regulation (GDPR) and Data Protection Act 2018 (DPA 2018) the University has an obligation to ensure the appropriate safeguards are in place when handling personal data.

1.3 Data security breaches are increasingly common occurrences whether these are caused accidently via human error or deliberately with malicious intent. As technology trends change and the creation of data and information grows, there are more emerging ways by which data can be breached.

1.4 The University needs to have in place a robust and systemic process of reporting and managing any incidents involving the breach of personal data.

A <u>Scope</u>

1.5 This University policy 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.

2. Definitions

2.1 The GDPR defines a "personal data breach" as a breach of security leading to the accidental or unlawful destruction, loss, alteration unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

2.2 It can be broadly defined as a security incident that has affected the confidentiality, integrity or availability pf personal data.

- Examples of data security breaches may include
- Loss or theft of data or equipment on which data is stored e.g. loss of laptop, USB stick or paper record.
- Unauthorised disclosure or Restricted/Confidential Data
- Equipment theft or failure
- Human Error
- Hacking attack
-

2.3 The GDPR only applies where there is a breach of **personal data.** For the purpose of this policy, not all security incidents are personal data breaches, all personal data breaches are security incidents. Any security breaches concerning personal data **confirmed or suspected** should follow this policy.

2.4 " Controller" The Controller determines the purposes for which and the means by which personal data is processed.

Information that the University is not the 'Controller" or Processor of, such as documentation brought on to Campus by students, that is subsequently lost and retrieved by University staff members will not constitute a data breach. This will be handled in accordance with the lost property policy/procedure.

3. Aim

3.1 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 authorized personnel, and consideration given to the referral to the Information commissioners/ 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 scrutiny.
- The notification of any data subjects and or external bodes where appropriate.
- The impact of incidents and actions taken to prevent reoccurrence and identify improvements in policies and procedures.

4. Responsibilities

4.1 The **University Leadership Team (ULT)** has overall responsibility to ensure that the University meets its legal and regulatory obligations.

4.2 **The Data Protection Officer (DPO)** has responsibility to brief and escalate data breaches where necessary to the Chief Compliance Officer & University Secretary for submission. The DPO will determine the necessity to report to the Information Commissioners Office/Supervisory authority and make recommendations.

4.3 **Heads of Departments/ System Owner/System Stewards** are responsible for ensuring that staff in their area act in compliance with the policy and provide appropriate assistance to investigations as required.

4.4 **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 incident reporting form (appendix1) and sending completed form to data.protection@hull.ac.uk , in the absence of the DPO the University Secretary and CSIRT@hull.ac.uk should also be informed.
- Assist with investigations as required and particularly if urgent action must be taken to prevent any further damage.

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

5. Containment & Recovery

Once the DPO has been notified they will undertake the following as required in the circumstances.

- Liaise with System Owner or Lead Officer where necessary and convene a breach response team to carry out investigations /actions if necessary
- Take Steps to contain the breach and take any immediate steps to prevent any further breach which may require input form specialist departments such as HR, Communications and HR.
- The relevant parties should be notified in a timely manner to ensure it is given the priority and action required.
- Conduct assessment of severity, risk and harm to individuals.
- Consider notification of relevant third parties and those individuals impacted.
- Record the breach and the management plan of the breach actions and results.

6. Notification of Breach

6.1 The University has a duty to report to the Information Commissioner Office (ICO) a personal data breach that is likely to result in **high risk** to the Rights and freedoms of individuals within 72 hours.

6.2 If the assessment of risk and impact identifies that the breach meets the threshold for referral the DPO will liaise with the CCO or SIRO and report the notifiable breach to the ICO/ Supervisory Authority either via telephone or via the online reporting form.

7. Evaluation & Response

7.1 Following every incident of a personal data breach it is important to investigate causes and evaluate our response to it. Existing controls will be reviewed to ensure adequacy and any changes required to policies and procedures.

7.2 To simply contain and continue business as usual is not acceptable and incidents will be reported on and follow up actions undertaken to minimize the risk of a similar incident reoccurring in the future.

A Appendix 1 - Incident Reporting Form

UNIVERSITY OF HULL

Version Control

Version	Author	Date approved	Relevant sections
V.3	A. Clement		

UNIVERSITY OF HULL

Appendix 1 Data Breach Incident Reporting form.

All individuals working for the University or handling personal data on behalf of the University are required to adhere to the Data Protection & Data Breach Policy and be aware of obligations and procedures in the event of a data security breach for reporting as soon as possible.

- Incidents and breaches **must** be reported immediately to your line manager and to the Data Protection Officer.
- This form where possible must be completed and emailed to dataprotection@hull.ac.uk as soon as the Data breach actual or suspected has been identified - the University is required to report **relevant** data breaches to the ICO within 72 hours.
- **Out of Hours** – The fully completed form should also be sent to the University secretary and CSIRT@hull.ac.uk
- **Please see guidance section overleaf to complete this form.**

Data and Time of Breach / Incident	
Faculty/ Department	
Description of the Breach / Incident and how it occurred	**(see guidance note 2)**
If a Data Breach has occurred - please mark all categories that were included in the breach	☐ Basic personal Identifiers e.g. name, contact details ☐ Identification data – e.g. usernames, passwords ☐ Economic / Financial Data e.g. Bank Details ☐ Health Data ☐ Location Data ☐ Criminal Convictions / Offences ☐ Trade Union Membership ☐ Official Documents e.g. Driving Licence ☐ Sex Life Data ☐ Genetic or Biometric Data ☐ Political Opinions ☐ Not yet known ☐ Any of the 9 Protected Characteristic Groups **(see guidance Section 3)** – Please State: ☐ Other - please state:
How many data subjects have been affected?	Number **Categories (Please see guidance section 4)**
Number of personal data records concerned (if applicable)	
Describe, identify any potential risks and impact to the affected data subjects(s) given the sensitivity of the data and any other risks identified.	**(See guidance section 5)**
What actions have already been taken to recover the breach or mitigate the risk	**(see guidance section 6)**
Have the data subjects been made aware? If so when and by whom?	
Type of Breach	**(see guidance section 7)**
Person Completing this form: • Name/Job Title • Date & Time Completed	

UNIVERSITY OF HULL

Guidance for Completing a Data Breach Incident Notification Report

Please work through the form and complete ALL sections.

1. What is a Personal Data Breach?

- **Personal Data** is defined as anything that can identify a real person
- A **Personal Data Breach** means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.
- This includes breaches that are the result of both accidental and deliberate causes.
- It also means that a breach is more than just about losing personal data.

2. Breach Descriptions and Occurrence Considerations

- Things to include in the description of the breach are who committed the breach / identified the incident
- What is the name of the individuals supervisor and what date / time were they notified
- What exactly happened (e.g., email sent to the wrong recipient, loss of keys, information etc.)
- Has the data breach spread further (did the email get forwarded to anyone else)
- Was it Human or System error
- Has it happened before If so when and what happened.
- If it is a ID card loss - have you contacted Estates
- If IT related incident – has ITCD been updated
- This is not an exhaustive list, please include all information

3. Protected Characteristics

Please identify all categories of protected characteristics that are in the data breach:

- Age, Race, Disability, Sex (Gender), Sexual Orientation, Religion or belief, Transgender, Pregnancy and Maternity, Marriage and Civil Partnership.

4. Data Subject Categories

Please identify all categories of data subjects are that have been affected by the breach / incident:

- Employees
- Students
- Children
- Vulnerable Adults
- Customers – this includes individuals requesting services or information from us e.g., Agents, applicants, alumni, etc.
- Research participants

5. What is a Potential or Real risk?

- Physical or emotional, material or non-material damage or distress caused or likely to be caused to any affected individuals.
- Could the breach lead to identity fraud, or any financial loss, or damage to a person's reputation or may lead to any economic or social disadvantage to a person(s) etc.?

6. Suggest actions to Recover or Mitigate the Breach

- For email breaches –
  - Try to recall the message using the outlook recall action
  - If you are unable to recall the email, contact ICT Support Desk to ask if they are able to recall it.
  - Send a follow up email to the recipient to request deletion, using the following statement:

'You have been sent an email in error from my contact address. You are asked to disregard the content and delete the email immediately.

Please confirm in writing that the deletion has taken place and that the information has not been further shared or forwarded to anyone else.'

- Contact the recipient(s) direct and ask that the email is disregarded, seeking written confirmation of the above actions
- Update Dataprotection@hull.ac.uk of recovery actions taken.

- For other hardcopy or removable media breaches –
  - Seek to retrieve the paperwork or removable media immediately.
  - Ensure it has not been accessed or shared further. If the items have been found by an individual, request confirmation from them that they have not accessed, copied or shared further.
- It is important you act quickly, if necessary, liaise with supervision to avoid any delay in implementing remedial action.
- Contact DataProtection@hull.ac.uk for further advice and support.

7. Types of Breach

The University classifies the breaches into different types depending on the incident. Please see the below types and enter the relevant one on the form:

- **Data Loss** – Any loss of data including missing discs, usb memory sticks, paper files etc.
- **Inappropriate Disclosure** – Includes the accidental or deliberate sharing of information to the incorrect person / organisation, wrong emails or information provided about the wrong data subject. This
- **Unauthorised Access inc Cyber Incident** – The accessing or attempts to gain unauthorised access to data (both via computer, verbal or hardcopy) that is not for a legitimate purpose. Changes to a systems hardware, software without the Systems Owners consent or malicious disruption.
- **Procedural Concerns** – This is where a breach occurs however we have followed the current procedure and it is identified that the procedure may require review.
- **Data Theft** – Theft of laptops, discs, mobile phones, briefcases that contain information.