UNIVERSITY OF HULL

Breach Management Policy

Classification:	
Version Number:	1.0
Status:	Approved
Approved by (Board):	Senior Leadership Team
Approval Date:	30 January 2018
Effective from:	30 January 2018
Next Review Date:	30 January 2019
Document Author:	Information Governance
Document Owner:	Information Governance
Department/Contact:	dataprotection@hull.ac.uk
Summary:	This document outlines the University's policy on reporting breach of data protection and management of the incident.
Scope:	This policy applies to all University members
Collaborative provision:	
Assessment: (where relevant)	
Consultation: (where relevant)	
Relevant legal frameworks:	
Related documents:	'Data Protection Policy'
Published locations:	
Document Communication and Implementation Plan:	Available upon request.

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

Table of Contents

1. Introduction 3
2. Aim 3
3. Definition 3
4. Scope 4
5. Responsibilities 4
6. Data Classification 4
7. Data Security Breach Reporting ……..... 5
8. Breach management plan……..... 5
9. Authority……..... 5
10. Review……..... 5
11. Appendix 1…… 6
12. Appendix 2…… 7

1. Introduction

Data security breaches are increasingly common occurrences whether these are caused through human error or via 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. The University needs to have in place a robust and systematic process for responding to any reported data security breach, to ensure it can act responsibly and protect its information assets as far as possible.

2. Aim

The aim of this policy is to standardise the University-wide response to any reported data breach incident, and ensure that they are appropriately logged and managed this will be achieved by adopting a standardised consistent approach to all reported incidents it aims to ensure that:

- incidents are reported in a timely manner and can be properly investigated
- incidents are handled by appropriately authorised and skilled personnel
- appropriate levels of University management are involved in response management
- incidents are recorded and documented
- the impact of the incidents are understood and action is taken to prevent further damage
- evidence is gathered, recorded and maintained in a form that will withstand internal and external scrutiny
- external bodies or data subjects are informed as required
- the incidents are dealt with in a timely manner and normal operations restored
- the incidents are reviewed to identify improvements in policies and procedures.

3. Definition

A data security breach is considered to be “any loss of, or unauthorised access to, University data”.

Examples of data security breaches may include:

- Loss or theft of data or equipment on which data is stored
- Unauthorised access to confidential or highly confidential University data
- Equipment failure
- Human error
- Unforeseen circumstances such as a fire or flood
- Hacking attack

- ‘Blagging’ offences where information is obtained by deceit

For the purposes of this policy data security breaches include both confirmed and suspected incidents.

4. Scope

This University-wide policy applies to all University information, regardless of format, and is applicable to all staff, students, visitors, contractors and data processors acting on behalf of the University. It is to be read in conjunction with the University Information Security Policy and Data Protection Policy.

5. Responsibilities

5.1 Information users

All information users are responsible for reporting actual, suspected, threatened or potential information security incidents and for assisting with investigations as required, particularly if urgent action must be taken to prevent further damage.

5.2 Heads of School/Department

Heads of Departments and School are responsible for ensuring that staff in their area act in compliance with this policy and assist with investigations as required.

5.3 Contact Details

The Information Office Compliance , who will be investigating breaches and suspected breaches can be contacted via dataprotection@hull.ac.uk

6. Data Classification

Data security breaches will vary in impact and risk depending on the content and the quantity of the data involved, therefore it is important that the University is able to quickly identify the classification of the data and respond to all reported incidents in a timely and thorough manner.

6.1 Public Data

Information intended for public use, or information which can be made public without any negative impact for the University

6.2 Internal Data:

Information regarding the day-to-day business and academic operations of the University. Primarily for staff and student use, though some information may be useful to third parties who work with the University.

6.3 Restricted Data:

Information of a more sensitive nature for the business and academic operations of the University, representing the basic intellectual capital and knowledge. Access should be limited to only those people that need to know as part of their role within the University.

6.4 Confidential Data

Information that, if released, will cause significant damage to the University's business activities or reputation, or would lead to breach of the Data Protection Act. Access to this information should be highly restricted.

7. Data Security Breach Reporting

Confirmed or suspected data security breaches should be reported promptly to the Information Compliance Department, email: dataprotection@hull.ac.uk The report should include full and accurate details of the incident including who is reporting the incident and what classification of data is involved. Where possible the incident report form should be completed as part of the reporting process. See **Appendix 1.**
Once a data breach has been reported an initial assessment will be made to establish the severity of the breach and who the lead responsible officer to lead should be.

All data security breaches will be centrally logged by the Information Compliance Department to ensure appropriate oversight in the types and frequency of confirmed incidents for management and reporting purposes.

8. Data Breach Management Plan

The management response to any reported data security breach will involve the following four elements. See **Appendix 2** for Investigation pro-forma
A. Containment and Recovery
B. Assessment of Risks
C. Consideration of Further Notification
D. Evaluation and Response

9. Authority

Staff, students, contractors, consultants, visitors and guests who act in breach of this policy, or who do not act to implement it, may be subject to disciplinary procedures or other appropriate sanctions.

10. Review

The Information Compliance Department will monitor the effectiveness of this policy and carry out regular reviews of all reported breaches.

11. Appendix 1

Incident Reporting Form

Please act promptly to report any data breaches (or potential data breaches/near miss). If you discover a data breach or near miss please notify your head of department and complete and return the form below to the information compliance team.

Description of Data Breach:	
Time and Date breach was identified and by whom:	
Date(s) when incident occurred	
Who is reporting the breach Name/post/department	
Contact Details of person reporting the incident Email address/phone number	
Classification of data breached (in accordance with the universities breach policy) **i. Public data** **ii. Internal data** **iii. Restricted Data** **iv. Confidential Data**	
Volume of data involved (number of people effected)	
Confirmed or suspected breach	
Is the breach contained or ongoing?	
What actions are being/have been taken to recover the data	
Who has been informed of the breach	
Any other relevant information	

Email this form to the Information Compliance Team at dataprotection@hull.ac.uk

Received by:	
Date/Time	

12. Appendix 2

Breach Management Plan

To be completed by the Information Compliance Office in consultation with the Head of area affected by the breach and if appropriate IT where applicable

Details of the IT systems, equipment, devices, records involved in the security breach:	
Details of information loss:	
What is the nature of the information lost?	
How much data has been lost? If laptop lost/stolen: how recently was the laptop backed up onto central IT systems?	
Is the information unique? Will its loss have adverse operational, research, financial legal, liability or reputational consequences for the University or third parties?	
How many data subjects are affected?	
Is the data bound by any contractual security arrangements?	
What is the nature of the sensitivity of the data? Please provide details of any types of information that fall into any of the following categories:	
HIGH RISK personal data **□ Sensitive personal data (as defined in the Data Protection Act) relating to a living, identifiable individual's** **a) racial or ethnic origin;** **b) political opinions or religious or philosophical beliefs;** **c) membership of a trade union;** **d) physical or mental health or condition or sexual life;** **e) commission or alleged commission of any offence, or** **f) proceedings for an offence committed or alleged to have been committed by the data subject, the disposal of such proceedings or the sentence of any court in such proceedings**	
Information that could be used to commit identity fraud such as; personal bank account and other financial information; national identifiers, such as	

National Insurance Number and copies of passports and visas;	
Personal information relating to vulnerable adults and children;	
Detailed profiles of individuals including information about work performance, salaries or personal life that would cause significant damage or distress to that person if disclosed;	
Spreadsheets of marks or grades obtained by students, information about individual cases of student discipline or sensitive negotiations which could adversely affect individuals.	
Security information that would compromise the safety of individuals if disclosed.	
Data Protection Officer and/or Lead Investigation Officer to consider whether it should be escalated to the appropriate University Executive Committee member	

Step 3 Action Taken

To be completed by Data Protection Officer and/or Lead Investigation Officer

Incident number	EG 01/2018
Report received by:	
On (date):	
Action taken by responsible officer/s:	
Was incident reported to Police?	Yes/No If YES, on what date
Follow up action required/recommended:	
Reported to Data Protection Officer and Lead Officer on (date):	
Reported to other internal stakeholders (details, dates):	

For use of Data Protection Officer and/or Lead Officer	
Notification to ICO	YES/NO If YES, notified on: Details:
Notification to data subjects	YES/NO If YES, notified on: Details:
Notification to other external, regulator/stakeholder	YES/NO If YES, notified on: Details:

Step 4 Data Breach Checklist to be considered by the Information Compliance Office

This checklist is not exhaustive and is a tool to ensure all information necessary to complete a full investigation is gathered.

This checklist will cover the 4 key areas in the event of a data breach

A. Containment and Recovery
B. Assessment of Risks
C. Consideration of Further Notification
D. Evaluation and Response

Step	Action	Notes
A	**Containment and Recovery:**	**To contain any breach, to limit further damage as far as possible and to seek to recover any lost data.**
1	Information Compliance Office to ascertain the severity of the breach and determine if any personal data is involved.	
2	Information Compliance Office to identify Lead Responsible Officer for investigating breach and forward a copy of the data breach report	To oversee full investigation and produce report. Ensure lead has appropriate resources including sufficient time and authority. If personal data has been breached also contact Br-Data-Protection. In the event that the breach is severe, the University Incident Management Team will be contacted to lead the initial response.
3	Identify the cause of the breach and whether the breach has been contained? Ensure that any possibility of further data loss is removed or mitigated as far as possible	Establish what steps can or need to be taken to contain the breach from further data loss. Contact all relevant departments who may be able to assist in this process. This may involve actions such as taking systems offline or restricting access to systems to a very small number of staff until more is known about the incident.
4	Determine whether anything can be done to recover any losses and limit any damage that may be caused	E.g. physical recovery of data/equipment, or where data corrupted, through use of back-ups.
5	Where appropriate, the Lead Responsible Officer or nominee to inform the police.	E.g. stolen property, fraudulent activity, offence under Computer Misuse Act.
6	Ensure all key actions and decisions are logged and recorded on the timeline.	

Step B	Assessment of Risks	To identify and assess the ongoing risks that may be associated with the breach
1	What type and volume of data is involved?	Data Classification/volume of individual data etc
2	How sensitive is the data	Sensitive personal data? By virtue of definition within Data Protection Act (e.g. health record) or sensitive because of what might happen if misused (banking details).

3	What has happened to the data?	E.g. if data has been stolen, it could be used for purposes which are harmful to the individuals to whom the data relate; if it has been damaged, this poses a different type and level of risk.
4	If the data was lost/stolen, were there any protections in place to prevent access/misuse?	E.g. encryption of data/device.
5	If the data was damaged/corrupted /lost, were there protections in place to mitigate the impact of the loss?	E.g. back-up tapes/copies.
6	How many individuals' personal data are affected by breach?	
7	Who are the individuals whose data has been compromised?	Students, applicants, staff, customers, clients or suppliers?
8	What could the data tell a third party about the individual? Could it be misused?	Consider this regardless of what has happened to the data. Sensitive data could mean very little to an opportunistic laptop thief while the loss of apparently trivial snippets of information could help a determined fraudster build up a detailed picture of other people
9	Is there actual/potential harm that could come to any individuals?	E.g. are there risks to: physical safety; emotional wellbeing; reputation; finances; identify (theft/fraud from release of non-public identifiers); or a combination of these and other private aspects of their life?
10	Are there wider consequences to consider?	E.g. a risk to public health or loss of public confidence in an important service we provide?
11	Are there others who might advise on risks/courses of action?	E.g. If individuals' bank details have been lost, consider contacting the banks themselves for advice on anything they can do to help you prevent fraudulent use

Step C	**Consideration of Further Notification**	**Notification is to enable individuals who may have been affected to take steps to protect themselves or allow the regulatory bodies to perform their functions.**
1	Are there any legal, contractual or regulatory requirements to notify?	E.g.: terms of funding; contractual obligations
2	Can notification help the University meet its security obligations under the seventh data protection principle?	E.g. prevent any unauthorised access, use or damage to the information or loss of it

3	Can notification help the individual?	Could individuals act on the information provided to mitigate risks (e.g. by changing a password or monitoring their account)?
4	Consider the dangers of 'over notifying'.	Not every incident will warrant notification "and notifying a whole 2 million strong customer base of an issue affecting only 2,000 customers may well cause disproportionate enquiries and work".
5	Consider whom to notify, what you will tell them and how you will communicate the message	There are a number of different ways to notify those affected so consider using the most appropriate one. Always bear in mind the security of the medium as well as the urgency of the situation. Include a description of how and when the breach occurred and what data was involved. Include details of what has already been done to respond to the risks posed by the breach. When notifying individuals give specific and clear advice on the steps they can take to protect themselves and also what the institution is willing to do to help them. Provide a way in which they can contact us for further information or to ask questions about what has occurred (e.g. a contact name, helpline number or a web page).
6	Consult the ICO guidance on when and how to notify it about breaches.	Where there is little risk that individuals would suffer significant detriment, there is no need to report. There should be a presumption to report to the ICO where a large volume of personal data is concerned and there is a real risk of individuals suffering some harm. Cases must be considered on their own merits and there is no precise rule as to what constitutes a large volume of personal data. Guidance available from http://www.ico.gov.uk/ for_organisations/data_protection/ the_guide/principle_7.aspx
7	Consider, as necessary, the need to notify any third parties who can assist in helping or mitigating the impact on individuals.	E.g. police, insurers, professional bodies, funders, trade unions, website/system owners, bank/credit card companies.

Step D	**Evaluation and Response**	**To evaluate the effectiveness of the University's response to the breach.**
1	Establish where any present or future risks lie.	
2	Consider the data and contexts involved.	E.g. what data is held, its extent, sensitivity, where and how it is stored, how long it is kept.
3	Consider and identify any weak points in existing security measures and procedures.	E.g. in relation to methods of storage and/or transmission, use of storage

		devices, levels of access, systems/network protections.
4	Consider and identify any weak points in levels of security awareness/training.	Fill any gaps through training or tailored advice.
5	Report on findings and implement recommendations	Report to Information Governance Working Group.