PRIFYSGOL BANGOR UNIVERSITY

PROCEDURES FOR THE MANAGEMENT OF A SUSPECTED DATA PROTECTION BREACH

Date	Purpose of Issue/Description of Change	Equality Impact Assessment Completed
5th October, 2009	Initial Issue	
16th July, 2018	Review and update	

Policy Officer	Senior Responsible Officer	Approved By	Date
Head of Compliance	University Secretary	Compliance Task Group	16th July, 2018

This Policy will be reviewed in 1 year

PROCEDURES FOR THE MANAGEMENT OF A SUSPECTED DATA PROTECTION BREACH

1. Introduction

It is mandatory, under the requirements of the Data Protection Act 2018, to report a data protection breach if it is likely to result in a risk to people's rights and freedoms. A notifiable breach must be reported to the Information Commissioner's Office within 72 hours of the University becoming aware of it.

The University must therefore take appropriate measures against unauthorised or unlawful processing and against accidental loss, destruction of or damage to personal data.

These procedures set out how the University will manage a report of a suspected data protection breach. Failure to report a breach when required to do so could result in a fine for delay, as well as a fine for the breach itself.

A data breach can happen for a number of reasons:

- Loss or theft of data or equipment on which data is stored
- Inappropriate access controls allowing unauthorised use
- Equipment failure
- Human error
- Unforeseen circumstances such as a fire or flood
- Hacking attack
- 'Blagging' offences where information is obtained by deceiving the organisation who holds it

In managing any report of a suspected data protection breach the University will take three distinct steps:

- Containment and Recovery
- Assessment of Risks and Further Notification
- Evaluation and Response

2. Reporting a Data Protection Breach

Any suspected data breach must be reported to the Head of Governance and Compliance, or the University Secretary, at the earliest possible opportunity and certainly within 24 hours so that appropriate containment and recovery action can be undertaken.

3. Containment and Recovery

Suspected data breaches require the University to investigate and contain the situation and also draw up a recover plan which will include where necessary any damage limitation.

On being informed of a suspected data breach the Head of Governance and Compliance will take the necessary steps to investigate, and will:

- Establish who needs to be made aware of the breach and inform them of what they are expected to do to assist in the containment exercise. (This may include, for example, isolating or closing a compromised section of the network, taking steps to find a lost piece of equipment or changing the access codes on a door);
- Establish whether there is anything to be done to recover any losses and limit the damage the breach could cause;
- Where appropriate, inform the police

4. Assessment of Risks and Further Notification

Before deciding on what further steps are necessary beyond those taken to immediately contain the breach the University Secretary and the Head of Governance and Compliance will, on behalf of the University, in consultation with the relevant Dean of College, Head of School and / or Director of Professional Service, undertake an initial assessment of the risks which may be associated with the breach.

As part of this assessment process consideration should be given to whether the incident requires notification to the Information Commissioner's office. In making this assessment the following factors will be considered:

- What type of data is involved?
- How sensitive is it?
- If data has been lost or stolen, are there any protections in place such as encryption?
- What has happened to the data?
- What could the data tell a third party about the individual?
- How many individuals' personal data are affected by the breach?
- Who are the individuals whose data has been breached?
- What harm can come to those individuals? Are there risks to physical safety or reputation, of financial loss or a combination of these and other aspects of their life?
- Are there wider consequences to consider such as a risk to public health or loss of public confidence?
- Is the breach likely to cause an individual to suffer some form of potential adverse consequence?

An assessment of potential adverse consequences for individuals, how serious or substantial these are and how likely they are to happen (e.g. financial loss, identity theft or a confidentiality breach) should also include consideration of the following factors, including notification to the individual themselves:

- Are there any legal or contractual requirements?
- Can notifying the individual help the University meet its security obligations with regard to the sixth data protection principle?[1]
- Can notification help the individual manage the risks for example by cancelling a credit card or changing a password?
- How can notification can be made appropriate for particular groups of individuals, for example, children or vulnerable adults.
- Who will the University notify, what will they be told and how will the message be communicated?
- Who else should be notified, for example third parties such as the police, insurers, professional bodies, bank or credit card companies.

The Head of Governance and Compliance will, at the conclusion of this stage, write a full report of the assessment processes undertaken to date, which will be presented to the Evaluation Group as outlined in Section 5 below.

If it is decided that the incident requires notification to the Information Commissioner's Office this should be done by the Head of Governance and Compliance at the conclusion of this stage, and in any event within 72 hours of being notified of the breach.

[1] Processed in a manner that ensures appropriate security of the personal data

5. Evaluation and Response

The University acknowledges that it is important not only to investigate the causes of any breach but also to consider the effectiveness of the University's response.

The Head of Governance and Compliance will therefore convene an *Evaluation Group* with a core composition including:

- The Chair of the Compliance Task Group who will become Chair of the Evaluation Group
- The Head of Governance and Compliance
- Relevant Dean of College, Head of Professional Service and / or Head of School determined by the nature of the breach
- Relevant operational managers determined by the nature of breach

The Evaluation Group, in drawing together its conclusions, will take into account the following key issues, in relation to the data breach:-

- • What are the lessons to be learnt?
- Can the University satisfy itself that it knows what personal data is held and where and how it is stored?
- In relation to personal data what and where are the biggest risks for the institution? For example where are special category data held?
- Are the risks associated with the sharing or disclosing of data suitably identified and managed?
- What are the potential weak points in the University's current security measures - such as the use of portable storage devices?
- How is staff awareness of security issues monitored, consider any gaps through training or tailored advice.

The Chair of the Evaluation Group will submit a full report to the Compliance Task Group at its next meeting, including any recommendations which may include action in accordance with the University's Disciplinary Procedures.