5th October, 2009	Initial Issue	
16th July, 2018	Review and update	
22nd September0 1 5		

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

Any suspected data breach must be reported to the Data Protection Officer, or the Head of Legal Services, at the earliest possible opportunity and certainly within 24 hours so that appropriate containment and recovery action can be undertaken. The contact details are as follows:
Email: info-compliance@bangor.ac.uk
Telephone: 01248 388525 or 388530

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 Data Protection Officer 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

Before deciding on what further steps are necessary beyond those taken to immediately contain the breach the Data Protection Officer will consult with the Head of Legal Services and the University Secretary / Head of Governance Services, 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

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

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.

In the event of a serious or repetitive breach, the Data Protection Officer 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 Services and / or the Head of Legal Services
- 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 Data Protection Officer

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