DATA BREACH MANAGEMENT PROCEDURE

1. Introduction

1.1 The University collects, holds, processes and shares large amounts of personal data and has an obligation to ensure that it is kept secure and appropriately protected.

2. Purpose

2.1 The purpose of this procedure is to ensure that:

personal data breaches are detected, reported, categorised and monitored consistently
incidents are assessed and responded to appropriately without undue delay
decisive action is taken to reduce the impact of a breach
improvements are implemented and communicated to prevent recurrence or future incidents
certain personal data breaches are reported to the Information Commissioner's Office (ICO) within 72 hours, where required

2.2 This document sets out the procedure to be followed to ensure a consistent and effective approach in managing personal data security breaches across the University.

3. Scope

3.1 This procedure applies to all staff, students, partner organisations and partner staff, suppliers, contractors, consultants, representatives and agents that work for or process, access, use or manage personal data on behalf of the University.

3.2 This procedure relates to all personal and special category ('sensitive') information handled, stored, processed or shared by the University whether organised and stored in physical or IT based record systems.

4. Definition

4.1 A personal data breach means ***s, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored***

4.2 A personal data breach in the context of this procedure is an event or action that has affected the confidentiality, integrity or availability of personal data, either accidentally or deliberately, that

Deliberate or accidental action (or inaction) by a data controller or processor

Sending personal data to an incorrect recipient

Alteration of personal data without permission

Loss of availability of personal data

Data input error / human error

Non-secure disposal of hardware or paperwork containing personal data

7.2 The Investigating Officer will investigate the breach and assess the risks associated with it, for example, the potential adverse consequences for individuals, how likely they are to happen and how serious or substantial they are.

7.3 The level of risk associated with a breach can vary depending on the type of data and its sensitivity. The investigation will need to consider the following:

What type of data is involved?

How sensitive is the data?

Where data has been lost or stolen are there any protections in place such as encryption?

What has happened to the data? Has it been lost or stolen?

Could the data be put to any illegal or inappropriate use?

Could it be used for purposes which are harmful to the individuals to whom the data relates?

How many individuals' personal data has been 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?

8. Notification of Breaches

8.1 The Investigating Officer in consultation with the Data Protection Officer, Head of Information Systems and Technology and Registrar, will determine who needs to be notified of the breach.

8.2 Any notification must be agreed by the Head of School/Centre/Department and Registrar.

8.3 Every incident will be assessed on a case by case basis. Not every

e

the categories and approximate number of personal data records concerned;

(b) the name and contact details of the data protection officer or other contact point where more information can be obtained;

(c) a description of the likely consequences of the personal data breach;

(d) details of the security measures and procedures in place at the time the breach occurred; and

(e) a description of the measures taken, or proposed to be taken, to deal with the personal data breach, including, where appropriate, the measures taken to mitigate any possible adverse effects.

8.4 If the University decides not to report the breach to the ICO it will need to be able to justify the decision and document it. Failing to notify a breach when required to do so can result in a significant fine up to *or* .

8.5 If a breach is likely to result in a high risk to the rights and freedoms of individuals, notification to the individuals whose personal data has been affected by the incident must be **without undue delay** describing:

the nature of the personal data breach;.24 599.38 Tm[(8.5)]TE9BT1 001 325.87 549.738 Tmc6(

9.1 Data protection breach management is a process of continual review. Once the initial incident is contained, the Data Protection Officer will carry out a full review of the causes of the breach; the effectiveness of the respons

APPENDIX 1

DATA BREACH REPORT FORM

Complete Section 1 of this form and email it to:

Data Protection Officer dpo@bolton.ac.uk
Head of Information Systems and Technology P.OReilly@bolton.ac.uk
Registrar s.duncan@bolton.ac.uk

Section 1: Notification of Data Security Breach To be completed by Head of School/Centre/Dept. of person reporting incident	
Date incident was discovered:	
Date(s) of incident:	
Place of incident:	
Name and contact details of person reporting incident (email, address, telephone number):	
Brief description of incident or details of the information lost:	
Number of people affected, if known:	
Has any personal data been placed at risk? If, so please provide details:	
Brief description of any action taken at the time of discovery:	
For use by the Data Protection Officer	
Received by:	
On (date):	
Forwarded for action to:	
On (date):	

Section 2: Assessment of Severity To be completed by the Investigating Officer with the Head of School/Centre/Dept. of the area affected by the breach and IT where applicable	
Details of the IT systems, equipment, devices, records involved in the security breach: Details of inf	

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;
Spread