DATA BREACH INCIDENT MANAGEMENT POLICY

1. Policy Statement

1.1 This guidance is intended to supplement the University of Wolverhampton ("the University") Data Protection and other information security policies, and has been developed in the aim of aiding the understanding of the University's obligations in the event of a data security breach.

1.2 These guidelines apply to all members of the University. All contractors and agents acting for or on behalf of the University should be made aware of these guidelines and the University's Data Protection Policy.

1.3 This policy applies to all methods of processing of personal information, on any device, whether University or personally owned, which is used for University purposes, whether, on a regular or an ad-hoc basis.

1.4 The General Data Protection Regulation and the Data Protection Bill require that personal data is processed fairly and lawfully and, in particular, not be used or processed in ways which would have unjustified adverse effects on the individuals concerned.

2. Breach of Data

2.1 A personal or sensitive data breach is a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed in connection with the purposes of the University business.

2.2 Members of staff at the University, who access, hold or process personal or sensitive data for the purposes of the University business must take appropriate steps to ensure no unauthorised or unlawful processing, accidental loss, destruction of, or damage to personal data occurs.

2.3 A personal data breach can occur for a number of reasons, such as:

a) Loss or theft of data or equipment on which data is stored;
b) Inappropriate access controls allowing unauthorised use;
c) Equipment failure;
d) Human error;
e) Unforeseen circumstances such as fire or flood;
f) Hacking attach;
g) Offences where information is obtained by deceiving the holder of the information, the University.

3. Containment and recovery

3.1 Data security breaches should be contained and responded to immediately upon discovering the breach. An Impact Assessment should be undertaken to identify measures required to contain or limit potential damage, and recover from the incident.

3.1 All data breaches, actual and potential, must be reported to the University Secretary, the Data Protection Officer (dataprotection@wlv.ac.uk) via the below Data Breach Incident Reporting Form and the IT Department, where appropriate.

4. Assessing the Risk

4.1 Some data security breaches may not lead to risks beyond possible inconvenience to those who need the data to undertake their role (i.e. a laptop is irreparably damaged, but its files were backed up and can be recovered). Following immediate containment, the risks must be assessed which may be associated with the breach, Potential adverse consequences to the individuals, as well as, the University itself, and the seriousness of the breach must be considered, further to immediate containment.

4.2 The following must be considered upon discovering a data breach:

a) The type of data involved;
b) Whether the data is sensitive
c) If data has been lost or stolen, whether encryption protections are in place;
d) What has happened to the data, such as the possibility that it may be used to cause harm to the individual(s);
e) The level of detail that would be exposed and how this could affect the individual

5. Notification of Data Breaches

5.1 Upon the completion of an Impact Assessment by the University Secretary or the Data Protection Officer, breaches capable of adversely affecting the individuals should be communicated to those individuals for the purposes of ensuring that specific and clear advice is provided on the steps to be taken to mitigate the risks and if any support could be provided.

5.2 It must be evaluated whether the Information Commissioner's Office, other regulatory bodies, and/or other third parties such as the Police or bank/building societies should be notified of the data breach.

5.3 Serious breaches may require for a 'media message' to be communicated to individuals concerned and the public at large, dependant on the seriousness and extent of the breach, which should be considered and implemented where appropriate.

6. Evaluation and Response

6.1 It is important that data breaches, actual or potential, are documented and investigated, and the response to the breach is evaluated in terms of its effectiveness.

6.2 Where a breach is caused by systematic and ongoing problems, merely containing the breach and continuing 'business as usual' will not be deemed acceptable. Areas requiring improvement for the purposes of preventing a re-occurrence should be identified and Policies and Procedures updated or implemented, as appropriate.

7. Additional Guidance

7.1 Additional guidance may be obtained from dataprotection@wlv.ac.uk

7.2 Related Policies:

a) Data Protection Policy
b) Acceptable Use of IT Facilities Policy
c) Encryption Policy
d) Document Retention Schedule
e) Information Security Policy
f) Password Policy

UNIVERSITY OF WOLVERHAMPTON

Data Breach Incident Reporting Form

NAME OF PERSON REPORTING:	**DATE OF BREACH OCCURRING:** **TIME:**	**DATE ON WHICH BREACH WAS DISCOVERED:** **TIME:**
SCHOOL/DEPARTMENT:		
EXTENSION NUMBER:		
DETAILS OF THE DATA BREACH		
How did the breach occur?	*Please provide as much information as possible:*	
Has a breach of this nature occurred before within the School/Department?	*If so, please provide dates of any previous breaches of the same nature:*	
How many individuals does the data breach affect?	*Please, aim to provide a figure as accurate as possible:*	
Are the individuals affected by the breach students/staff, or both?		
What data has been lost/stolen/compromised or else disclosed without the appropriate authority?	*i.e. CVs, Financial Information, Contact details etc.:*	
Whom was the data released to, if known?		
Is the data sensitive? YES/NO	*If YES, please provide a list of sensitive data concerned:*	
Are you aware of the individuals affected?	*If so, please provide their names and any contact details, where known:*	
What steps could those individuals take to protect themselves from any harm/risk arising from the breach?	*i.e. report to their bank/building society, report to the Police etc.:*	
Does the breach concern manual or electronic data, or both?		
Were encryption protections in place at the time of the breach?		

Have the IT Services been informed?	*If your account has been hacked, you must change your password immediately and report the incident to IT Services:*
Has the incident been reported to the Police or any other authorities?	*If so, please provide date of reporting and reference number:*
IS THERE ANYTHING ELSE THE UNIVERSITY SHOULD BE AWARE OF?	
Please comment below:	
THIS FORM MUST BE SUBMITTED TO dataprotection@wlv.ac.uk and the University Secretary.	

VERSION:	**1.1**	**AUTHOR/ OWNER:**	**Office of the University Secretary**
Approved Date:	May 2018	**Approved By:**	Board of Governors
Review Date:	May 2019		