Data Protection Incident Policy

Purpose

This Data Protection Incident Policy places obligations on staff to take appropriate measures to report potential breaches of personal data security and details the course of action to take upon their discovery.

Policy statement

London Metropolitan University maintain personal and sensitive data relating to our staff, students and organisation. As a Data Controller, the University has a responsibility under the Data Protection Act 1998 (DPA 1998) to protect the security of the personal data we hold. This duty requires us to put in place appropriate technical or organisational measures against the unauthorised or unlawful processing of personal data as well as protecting the data against accidental loss, destruction or damage.

In the event of a data protection incident our primary objectives are to:

- prevent the further spread/loss of data
- recover any data that has been lost
- identity risks arising from the incident/breach
- notify appropriate parties of the incident/breach
- prevent future incidents

Scope

This policy applies to all London Metropolitan University staff, and to all personal and sensitive data held by us. This policy supplements our policies relating to data protection, information security and other relevant policies.

Data protection incidents

A personal data security breach can be caused by criminal activity (eg theft, unauthorised access or sharing of data, hacking or phishing scams) or unintentional (eg accidental loss, deletion or damage of data, hardware failure, software corruption, human error or disaster such as fire or flood).

Actions upon discovery of an incident

All personal data breaches must be reported to your relevant line manager immediately upon discovery, or if discovered outside normal working hours then as soon as is reasonably practicable. Line managers must record the details of the

breach and inform the Information Compliance Officer of the breach. A questionnaire to assist with the collection of information about the breach is attached in the Appendix to this Policy.

Upon being informed of a possible breach, the Information Compliance Officer will, together with the University Secretary and Chief Information Officer, carry out an assessment of the actions necessary to mitigate harm that might result from the breach. Each breach will be assessed individually, and any actions taken shall be appropriate to the particular circumstances of the incident in question. Depending on the nature of the incident, the University's ITS Security Incident Handling Policy may also need to be invoked.

Any investigation should consider the following:

- Identify how the security breach occurred and immediately take steps to limit the spread of data and prevent a recurrence of the breach
- Identify ways to recover the data
- Confirm the amount, sensitivity and type of information in question
- Identify what security measures were in place when the breach occurred as well as what measures have been put in place following it
- Confirm who has been put at risk and assess the potential harm resulting from the breach
- Consider the additional consequences of the breach including loss of reputation, loss of business, liability for fines or contractual breaches
- Consider who to inform about the breach both internally within the organisation and externally (eg the Police, Information Commissioner, other regulatory authorities and individuals concerned)
- Consider whether notification is necessary and beneficial, and whether there would be any adverse consequences of informing third parties
- Determine the response to any media enquiries, in conjunction with the PR and Internal Communications Manager
- Assess data security risks and whether technical or organisational measures could be implemented to minimise these in future.

Implementation and review

This policy takes effect immediately upon publication and will be subject to a review 12 months after its implementation.

Contact information

The university's Information Compliance Officer can be contacted on 020 7133 4137 or by email at: dsar@londonmet.ac.uk

Date 28 March 2017

Name	
Position	
Contact details	
Date	
Line manager	
Line manager contact details	
Time/date of breach	
Time/date of discovery of breach	
Description of data involved	
Summary of incident	
Is breach ongoing?	
What steps have been taken to minimise the effects of the breach?	
Parties affected by the breach	
People notified of breach	
Signed:	
Name:	
Position:	
Date:	