Breach Reporting Policy

CONTENTS

CLAUSE

1.0 Purpose

This Policy sets forth the principles and requirements that govern Breach Reporting

2.0 Scope

This Policy applies to all individuals working at all levels and grades, including senior managers, officers, directors, employees (whether permanent, fixed-term or temporary), consultants, contractors, trainees, seconded staff, home employees, casual employees and agency staff, volunteers, interns, agents, sponsors or any other Associated Person with The University of Law ("ULaw")

3.0 Target Audience

The target audience is represented by the groups below:

Full Time Employees
Contractors/Temporary Part-Time Employees
Third-Party/Agency Staff

4.0 Applicable Laws and Regulations

This Policy is intended to be consistent with all applicable legal and regulatory requirements regarding their subject matter.

The following Laws and Regulations are applicable to this policy:

Data Protection Act 2018

5.0 Compliance with this Policy is measured by the following departments:

1. Data Protection - through continuous monitoring and review of policy content, as well as monitoring changes in regulations and regulatory interpretations in those countries in which such monitoring is the responsibility of the Data Protection Officer ("DPO").

2. Audit - through scheduled audits.

3. Policy Administration - through the annual policy review process.

The data protection team is accountable for the implementation of this policy. Any changes to this policy and any reviews of this policy are subject to approval by the ULaw Senior Management Team. All relevant ULaw Employees are accountable for the proper observance of this policy and its adjoining procedure. This Policy may be subject to review by an external auditing firm, examiners and governmental agencies.

6.0 Definitions

Definitions of significant terms used in this Policy are listed below:

Associated Person - a person who “performs a service” for or on behalf of the organisation. This person can be an individual or an unincorporated body. This can include employees, agents, subsidiaries, contractors and suppliers –

Breach - This is a failure to maintain a process, rule, law or regulation; a failure to obey, keep or preserve a law or to breach confidentiality.

ICO - Information Commissioner's Office

7.1 Breaches Procedures

All data breaches, actual and potential, must be reported immediately to the Data Protection Officer (by completing the Data Breach Incident Reporting Form (on page 7) and sending it to DPO@law.ac.uk as well as via the IT Department (where appropriate).

Data security breaches should be contained and reported to the DPO immediately upon discovering the breach. A Data Breach Incident Reporting Form (see page 7) should be completed to report and identify measures required to contain or limit potential damage and recovery from the incident. Once completed the form should be returned to DPO@law.ac.uk

Some data security breaches may not lead to risks beyond possible inconvenience to those who need the data to undertake their role (e.g.. a laptop is irreparably damaged, but its files were backed up and can be recovered). Once the breach has been contained, the risks that may be associated with the breach must be assessed, 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.

The following must be considered by the DPO upon discovering a data breach:

- Whether the data is sensitive.
- If data has been lost or stolen, whether encryption protections are in place.
- What has happened to the data, such as the possibility that it may be used to cause harm to the individual(s).
- The level of detail that would be exposed and how this could affect the individual.
- Upon the completion of a Data Breach Incident Reporting Form, the DPO may decide that the breach is capable of adversely affecting individuals and 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.

The DPO will evaluate 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.

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.

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.

8.0 Overview

The purpose of the Breach Reporting Policy is to ensure compliance with Regulatory requirements when there is a breach of internal policy and procedure, or suspected breach of UK, EU regulation or law within ULaw.

ULaw expects all employees to abide by this policy and accompanying procedure.

9.1 Responsibilities of the Employee

- Complete the Mandatory online Data Protection induction training.
- Be aware of the Breaches Policy and accompanying procedure.
- Report any breach of policies and procedures or suspected breach of UK or other applicable laws or regulations immediately to their Manager or equivalent senior staff member if their Manager is not available.
- Carry out remediation actions within the timescales set out in any remediation plan linked with a Breach as applicable.
- Not communicate with anyone about the breach apart from the Employee's Manager, the DPO and the Legal Team unless authorised to do so.

9.2 Responsibilities of the Manager

The Manager or their representative shall:

- Notify compliance of the Breach by following the Breach Procedure.
- Liaise with the employee DPO and legal where required, to assist in the remediation of the Breach.
- Agree with the DPO planned remediation deadline.
- Confirm the planned full remediation activity including anticipated completion dates within 3 working days (if not included in the initial Breach form).
- Notify the DPO if for any reason the remediation deadline will not be met as initially anticipated.
- Not communicate with anyone about the breach apart from those authorised by the DPO or the legal team.

9.3 Responsibility of the Data Protection Officer

- Upon receiving the breach notification form, via the assigned Manager, acknowledge the Breach.
- Add the incident to the internal Breach log.
- Immediately inform the Chief Operating Officer by email if necessary.
- Notify Legal.
- Liaise with legal and the Manager, as well as any business areas that may be affected or required to assist in the remedy of the breach, to establish a remediation plan or delegate this activity appropriately.
- Advise on the effectiveness and propriety of any remediation plan outlined.
- In conjunction with legal, make recommendations on when and/or how to contact the data subject, ICO or other affected party; in conjunction with Legal, review and approve any correspondence prior to its release to the affected parties.
- Seek updates from the business regarding the progress of the remediation.
- Provide a report outlining details of any open Breaches and Breaches that are repeated, serious or 30 days past the planned remediation date.

The Data Protection Team will only close the issue on the Breach log when all action items are closed and a written remediation affirmation has been provided by the business.

10 Serious Breaches

'Seriousness' should be determined by considering the number of Students/Clients/Employees affected, frequency of the Breach recurring, the involvement of regulatory bodies and if there were delays in identifying or rectifying the Breach.

The DPO must then notify a member of the Executive Team, once a Breach has been identified as falling into the 'Serious' category. The DPO will appoint an Event Team, with advice from legal and the COO, to preside over the Breach investigation. The Event Team will comprise of at least 2 Executives and representation from Legal and the DPO. The Event Team should discuss the Breach, the root causes, the impact and take the following decisions:

- Any remedial/preventative steps taken/ that remain.
- Ascertain the next steps forward.
- Whether this is to be notified to the customers.
- Whether the ICO is to be notified.
- Any legal steps.
- Any required report to the ICO is to be drafted by DPO/Legal and approved by the Event Team.
- The DPO is responsible for keeping the Event Team informed of the communication with the ICO and to report to the Event team. The DPO will only close the issue on the Breach log when all action items are closed and a remediation affirmation has been provided by the University.

Serious Breaches may require a ‘media message’ to be communicated to individuals concerned and the public at large, dependent on the seriousness and extent of the Breach, which should be considered and implemented where appropriate. The media message must be agreed by the DPO, legal and a member of the exec team before it is communicated. The marketing/communications team will deal exclusively with the DPO and the legal team in formulating the message unless authorised to consult elsewhere.

11.0 Communication

The DPO will communicate information regarding major changes in University strategy or the regulatory environment to the relevant recipients.

12.0 Training

Training shall be provided by the DPO and via eLearning and further training will be given periodically when any major changes occur as outlined above. Refresher training on the appropriate Breach procedures will be provided in line with training requirements.

Exceptions and Escalations - Any deviation from the minimum requirements set forth in ULaw Policies is exposing the University to risk. Thus, ULaw Policies must be reviewed annually by the Data Protection Officer and any appropriate Risk function (Executive Team, Legal, Data etc.).

Any request for an exception to this policy must be made to the DPO.

Data Breach Incident Reporting Form

NAME OF PERSON REPORTING: **DEPARTMENT:**	**DATE OF BREACH OCCURRING:** **TIME:**	**DATE ON WHICH BREACH WAS DISCOVERED:** **TIME:**
CONTACT 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 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 third Party? **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?	

Version	Date	Author	RevisionSummary
V 1.0	09/2020	DPO	

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 DPO@law.ac.uk	