Procedure for Notification of Data Security Breaches

Version Control

1. Full Document Number:	OPESOP001
2. Version number:	4.0
3. Superseded version number:	3.1
4. Document owner job title:	Data Protection Officer
5. Department / function:	Strategic Operations
6. Next review date:	01-APR-2024
7. Add document to external LSTM website?	Yes

Modifications from previous version of document

Version	Date of issue	Details of modification
3.0	04/2019	Fewer sections, clearer headings. Describe use of software and additional routes of reporting. More examples of breaches. Figure of the steps in the procedure. Summarised thresholds for reporting to ICO and to victims. Added link to European guidance.
3.1	21/05/2019	Typographical corrections following Governance Oversight Committee
4.0	03/2021	Office for Students notification. Adding links to online LSTM resources, e.g. Freedom to Speak Up, Microsoft Forms version of reporting form, breach team Teams group. Change wording from victim to data subject. Added risk assessment and criteria for meetings of breach team.

Contents

1 Scope

This policy applies to all staff and students processing personal data.

2 Introduction and Context

2.1 This document sets out the procedures for reporting of data breaches and:

2.1.1 places obligations on staff to report potential breaches of personal data protection; and

2.1.2 sets out the procedure for managing reported breaches.

2.2 This guidance applies to all staff, and to all personal data including special categories of personal data held by LSTM as defined by the Data Protection Act. This Procedure should be read in conjunction with guidance on the correct handling of personal data and the meaning of specialist terms found in:

the Data Protection Policy, and

the data protection section of the Knowledge Exchange.

3 Equality and Diversity

LSTM is committed to promoting equality of opportunity, combatting unlawful discrimination and promoting good community relations. We will not tolerate any form of unlawful discrimination or behaviour that undermines this commitment and is contrary to our equality policy.

4 Safeguarding

In line with our Safeguarding policy and procedures, LSTM's processes reflect our organisational commitment to keeping children and vulnerable adults safe.

5 Roles and Responsibilities

5.1 The Data Protection Officer is responsible for writing the procedure and obtaining sign-off.

5.2 The Governance Oversight Committee is responsible for approval of the procedure and monitoring compliance.

5.3 All staff who process personal data are responsible for

reading and applying the procedure, and

raising any queries or uncertainties with the Data Protection Officer to improve this procedure and its supporting guidance.

6 What is a data security breach?

6.1 LSTM processes personal data relating to individuals including staff, students and third parties. LSTM has a responsibility under the Data Protection Act 2018 to protect the security of personal data. We need to apply technical and organisation measures to keep personal data secure. All staff are required to comply with information security guidelines and policies including our Data Protection Policy, Information Classification Matrix and Acceptable Use of Computer & IT Facilities to be found on the Policy Hub.

6.2 A data breach is "a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed"[1].

6.3 Examples of data breaches are:

- loss or theft of data or equipment on which data is stored, e.g. loss of a laptop, USB stick or a paper file;
- unauthorised person gaining access to a filing cabinet, shared drive, or unlocked computer;
- failure of equipment that stores or handles personal data;
- human error, e.g. sending an email or fax to the wrong recipient;
- unforeseen circumstances interrupting services such as a fire or flood;
- hacking, phishing and other blagging attacks where information is obtained by deceiving whoever holds it, for example spoof telephone calls.

6.4 See Appendix 3 for detailed criteria and further examples

7 Reporting a potential breach

7.1 Once detected, the focus in responding to a breach is on protecting individuals and their personal data. Every breach or potential breach should be reported promptly and without delay to the Data Protection Officer. This triggers the further steps below, which ensure a proper and orderly response, help assess the risk to individuals and help us comply with our legal obligations.

[1] https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/personal-data-breaches/

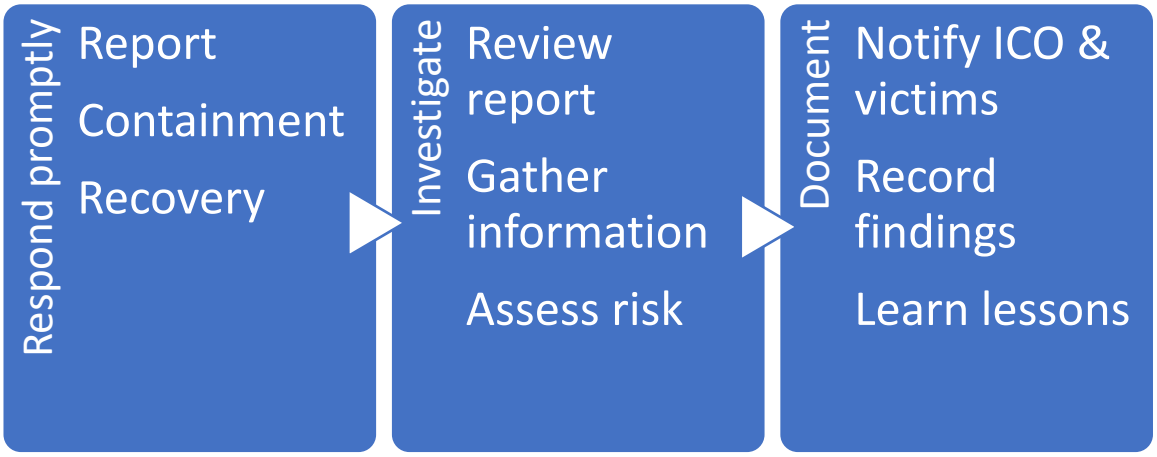

Figure 1 Steps to follow once you have detected or suspected that a breach may have occurred. The first step, which should be done without delay, is to report. The Data Breach Team take the lead on the following steps.

7.2 How to report a breach:

First, alert the Data Protection Team that a breach has occurred by emailing the data protection inbox dataprotection@lstmed.ac.uk or by calling the Data Protection Officer on +44 151 702 9323.

Further information should then be captured in communications with the Data Breach Team and by completing a breach report. This can be completed using the template downloadable from the Policy Hub which should be emailed to dataprotection@lstmed.ac.uk or by completing this online form.

If you prefer to report data protection concerns anonymously, please use the Freedom to Speak Up page (option 4).

7.3 Where appropriate, you should liaise with your line manager about completion of the report form. However, this may not always be appropriate, e.g. if your line manager is not available or if you have been instructed not to report the incident but you believe that it should be reported. In these circumstances, you should submit the report directly without consulting your line manager.

7.4 Monitoring of the dataprotection@lstmed.ac.uk email will be carried out by the Data Protection Officer and nominated deputies within the Data Breach Team (see Appendix 2).

7.5 You **should not take** any further action in relation to the breach, (for example contacting any affected individuals or regulators) unless advised by the DPO or

deputy or IT Services. The Data Breach Team will lead and coordinate all steps after you make the initial report.

7.6 All staff should be aware that contravention of obligations under the Data Protection Act 2018 could result in disciplinary action being taken under LSTM's Disciplinary Procedures. Any failure to report a data breach as defined in the LSTM Data Protection Policy and this accompanying Guidance document, could be classed as such a contravention.

8 Handling a breach report

8.1 On being notified of a suspected data security breach by IT Services, the DPO will assemble the Data Breach Team. In the first instance this will be done virtually, and if necessary a physical meeting arranged.

8.2 The Data Breach Team will be led by the DPO or a deputy (see Appendix 2).

8.3 The Data Breach Team will take immediate steps to establish whether a breach has occurred, and what appropriate action should be taken to:

contain the data breach and (so far as reasonably practicable) recover, rectify or delete the data that has been lost, damaged or disclosed;

assess and record the breach in LSTM's Data security breach register;

determine whether LSTM has also breached any duty of confidentiality owed to third parties by LSTM;

notify appropriate parties of the breach;

take steps to prevent future breaches.

9 Actions following a breach

9.1 Once a report is received, the following steps are to

contain and recover the breach as far as possible,

gather information and assess risk, and

notify appropriate parties of the breach

9.2 The Data Breach Team will work with the appropriate people in LSTM to identify how the security breach occurred and take immediate steps to stop or minimise further loss, destruction, or unauthorised disclosure of data. One such step could be forcing an immediate password change, but this will depend on the nature of the breach.

9.3 The Data Breach Team will work with the appropriate people in LSTM to identify ways to recover, correct or delete data. This may include contacting the police if the breach involves theft or forced entry or sending hardware to contracted data recovery experts if data on computer equipment is inaccessible.

9.4 Depending on the nature of the breach, the Data Breach Team will notify the LSTM's insurers.

9.5 The Data Breach Team will review the data breach report form and gather other information to objectively assess the risks associated with the breach, including the:

- type, volume, identifiability and sensitivity of data,
- number and type of individuals involved,
- protections around the data such as encryption,
- likely consequences of the breach on individuals, e.g. risks to physical safety, reputation, identity theft or financial loss, and
- likely consequences of the personal data breach for LSTM, e.g. reputational damage, loss of business, liability for fines, lack of trust in a service.

9.6 These findings should be recorded in LSTM's Data Breach Register.

9.7 The Data Breach Team will consider whether to notify:

affected data subjects;

the police;

the ICO;

any other parties, e.g. insurers, commercial partners, or other regulators.

In determining whether to notify affected data subjects, the Data Breach Team will have regard to the law and guidance from the ICO or other respected bodies (see Appendix 4). For example[2]:

Reporting to the ICO is mandatory unless there is unlikely to be a risk to the rights and freedoms of individuals.

Individuals must be informed if there is a likely high risk to their rights and freedoms.

9.8 Each data subject will be notified by email by the DPO where we have the victim's email address. BCC will be used to protect identities wherever there are multiple recipients. We will request that they acknowledge receipt of the message. The template notification will be used wherever relevant [See Appendix 3].

9.9 The police may be notified to assist with containment and recovery. If it subsequently transpires that the breach arose from a criminal act, the Data Breach Team will notify the police and/or relevant authorities, for example the National Cyber Security Centre.

[2] Guidelines on Personal data breach notification under Regulation 2016/679 (wp250rev.01) https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612052

9.10 Notifying the ICO. The Data Breach Team will decide whether to notify the ICO when LSTM is controller. Notifiable breaches put individual rights and freedoms at risk. LSTM is required to report all data breaches to the ICO within 72 hours. The ICO has a dedicated “Reporting a data breach” page https://ico.org.uk/for-organisations/report-a-breach/ and telephone line 0303 123 1113.

The only exceptions where the ICO does not need to be notified by LSTM are:

- when LSTM is not data controller; LSTM will instead need to notify and assist the controller who will notify their supervisory authority, and
- the personal data breach is **unlikely** to result in a risk to the rights and freedoms of individuals. If in doubt the controller should err on the side of caution and notify.

9.11 Notifying other parties. The Data Breach Team will consider whether there are any legal or contractual requirements to notify any other parties. When the data subjects are students, consideration should be made of whether to notify the Office for Students via https://www.officeforstudents.org.uk/for-students/notifications/

9.12 The outcome of these assessments will be reviewed by the Data Breach Team, recorded in the Breach Log, and lessons learned and actions arising shared with other LSTM staff as relevant.

Appendix 1: Data Breach Report Form

We no longer include a pdf copy of the Data Breach Report Form ISTTEM007. Please complete the Word document downloadable from the Policy Hub: https://lstmed.sharepoint.com/policies/PoliciesProcedures/Data%20Breach%20Report%20Form.docx or the version on Microsoft Forms: https://forms.office.com/Pages/ResponsePage.aspx?id=yQ1AlSA5YEykGP68wJ74Wg9HZ51ELdxEm5HJd1k5MyJUN09JOE1IVllWWFBQUUlIRURUSUNWRFQwSy4u

Appendix 2: Data Breach Team

Staff with the following job titles are members of the Data Breach Team and all have access to the software used to record data breaches:

- Data Protection Officer
- Director of Strategic Operations, International & UK
- Head of Information Services
- Head of IT
- IT Operations Manager
- Group Legal and IP Advisor
- Director of Strategic Projects
- Deputy DPO (Governance Manager – Monitoring, Risk and Audit)
- Deputy DPO (Head of Corporate Performance and Information Planning)

A meeting of the Data Breach Group will be triggered when the report information available indicates three or more of the following apply:

Special category data have been breached

Numbers of affected data subjects is greater than 10

IT system integrity is threatened

Significant reputational risk from the data breach

Data could be used for identity fraud

Significant financial risk to the data subjects from the breach

Meetings of the Data Breach Team must consist of at least 4 of the following including the Data Protection Officer (or a deputy), a member of IT Services and the Director of Strategic Operations, International & UK. In addition, the individual reporting the breach may attend accompanied by their Director of Studies if a student or their line manager or head of department if a member of staff.

Meetings will have at least these three aims: (1) establishing the facts around the breach, (2) summarising lessons learned from the breach, (3) determining a plan of action.

Appendix 3: Data breach risk criteria

The following guidance summarises European guidelines on breach reporting[3], and draws on recent LSTM experience.

Breaches disrupt the confidentiality, integrity, or availability of personal data. They are diverse and no list is exhaustive; some examples are described in Table 1.

Table 1 Types of breach, their definition, what they might look like at LSTM, and exemptions of routine work that does not constitute a breach.

Type of breach	Definition	Examples	Exemptions
Destruction	Data no longer exists in a form that is of any use to the controller	Ransomware scrambles personal data on a device Encryption keys corrupted, resulting in entire volume and backups being unreadable	Planned destruction in line with retention schedule
Damage	Data are altered, corrupted, or incomplete	Forms are sent in the post but only some arrive Device for data collection is wiped leaving the project with only part of their dataset	Some data items are purposely made unavailable for scientific control e.g. blinding in clinical trial Cryptographic keys destroyed as part of anonymisation work so that codes cannot be reversed
Loss	Losing control or access to data (even if temporary)	Power failure or DDoS attack means personal data system unavailable USB stick misplaced	Outage is planned maintenance or only causes a few minutes disruption to noncritical services
Unlawful processing	Disclosure of data to those not authorised to view it	Intruder hacks into LSTM network Printer hard drive not wiped before being sold Data from one project shared with collaborator for another purpose without ethical approval	Intruder views encrypted personal data and does not have encryption key Right processes followed for disclosure or repurposing of personal data

Any breach should be reported immediately (see section 7 Reporting a potential breach), and the likelihood and severity of impact on individuals identified in the data will subsequently be assessed by the Data Breach Team.

All possible consequences of a breach should be considered. Potential risks may have been documented in the Data Protection Impact Assessment. These encompass physical, material, or non-material risks and could include:

Loss of control over their personal data

[3] Guidelines on Personal data breach notification under Regulation 2016/679 (wp250rev.01) https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612052

Limitation of their rights

Discrimination

Identity theft or fraud

Financial loss

Unauthorised reversal of pseudonymisation

Damage to reputation

Loss of confidentiality of personal data protected by professional secrecy

Other significant economic or social disadvantage

The likelihood and severity of these consequences can depend on:

The type of breach

Nature, sensitivity, and volume of data

Number of affected individuals

Ease of identification of individuals

Severity of consequences for individuals

Special characteristics of individuals or of the controller

The severity and likelihood of the assessed risks should be scored and the result recorded in the data breach log. The method of two scores ranging from 1 to 5 outlined below is based on NHS Data Security Standard 6. We should inform the ICO if one of the scores is 3 or above, unless the data are encrypted, recovered or the effect can be otherwise nullified.

Severity score - Significance of consequences:

1 - lowest, no adverse effect

2 – potentially minor effect

3 – potential adverse effect (report to ICO, consider notifying individuals)

4 – potentially pain and suffering/financial loss (report to ICO, notify individuals)

5 – death or catastrophic event (report to ICO, notify individuals)

Likelihood score – Probability of consequences occurring:

1 - non-occurrence

2 – not likely

3 – likely (report to ICO, consider notifying individuals)

4 – highly likely (report to ICO, notify individuals)

5 - has occurred (report to ICO, notify individuals)

The following objective questions may assist with derivation of the above scores (informed by Article 29 working party guidance 2016/679).

Who is involved?

- Are the data subjects a vulnerable group? Both scores 2 or above
- Data in the hands of people with malicious intent? Severity 2 or above, likelihood 3 or above
- Does this threaten an organisation's duty of confidentiality?

What types of data are involved?

- If just name and address then disclosure is usually unlikely to cause substantial damage (Both scores 1) unless subjects are part of a vulnerable group
- Are special category data involved? Likelihood 3 or above
- Financial data or identity documents? Could be used for identity theft – Significance=4 or above

Appendix 4: Notification to data subject

Notification of a Data Breach

What happened?

What information was involved?

What we are doing

What you should do

Any other details

For further information contact:

Data Protection Officer: dataprotection@lstmed.ac.uk 0151 702 9323