



## **DATA BREACH POLICY**

April 2025



# DATA BREACH POLICY

## CONTENTS

1.0	INTRODUCTION.....	1
2.0	AIMS.....	1
3.0	MONITOR AND REVIEW .....	1
4.0	EQUAL OPPORTUNITIES.....	1
5.0	RESPONSIBILITY FOR THIS POLICY .....	2
6.0	ACTION TO BE TAKEN IN THE EVENT OF A DATA BREACH .....	2
7.0	CONTROL AND RECOVERY.....	2
8.0	ASSESS THE RISK.....	2
9.0	NOTIFYING THE INFORMATION COMMISSIONER.....	3
10.0	EVALUATION AND RESPONSE.....	3

## 1.0 INTRODUCTION

---

- 1.1 Lothian Valuation Joint Board (LVJB) is required under Data Protection Laws to ensure the security and confidentiality of all personal and sensitive personal data it processes. Every care should be taken by staff to protect the personal data they work with and to avoid the unauthorised disclosure or loss of any personal data.

## 2.0 AIMS

---

- 2.1 This policy applies to all personal and sensitive personal data processed by the LVJB and is concerned with the Security Principle as defined in Chapter II, Article 5(1), (f) of the General Data Protection Regulation (GDPR):

*'Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures'*

- 2.2 Potential examples of a personal data breach could include:

- personal data accidentally being sent to someone (either internally or externally) who does not have a legitimate need to see it;
- databases containing personal data being compromised, for example being illegally accessed by individuals outside the LVJB;
- computing devices containing personal data being lost or stolen;
- paper records containing personal data being left unprotected for anyone to see, for example files left out when the owner is away from their desk, papers not properly disposed of in secure disposal bins that can then be extracted or seen by others or papers left at photocopyers;
- alteration of personal data without permission;
- access by an unauthorised third party.

## 3.0 MONITOR AND REVIEW

---

- 3.1 This Policy has been created and will be maintained in accordance with the LVJB Policy Approval Framework. It has been agreed by CLT (and the Board as required), in consultation with the Trade Union where appropriate.
- 3.2 ICT is responsible for monitoring the effectiveness of this Policy and supporting procedures and will conduct reviews at appropriate intervals.

## 4.0 EQUAL OPPORTUNITIES

---

- 4.1 LVJB is committed to equality of opportunity for all its employees and the terms of this Policy and its supporting procedures and guidance notes are designed to ensure the fair and transparent treatment for all staff irrespective of age, race, disability, gender reassignment, marriage and civil partnership, pregnancy and maternity, sexual orientation, religion or belief, gender or contractual status. An Equality Impact Assessment is undertaken on this Policy each time it is reviewed and updated.

## 5.0 RESPONSIBILITY FOR THIS POLICY

---

Responsibility for the implementation and annual review of this policy together with the communication of any resultant amendments across the organisation and to relevant third parties is assigned to the ICT Support Manager

## 6.0 ACTION TO BE TAKEN IN THE EVENT OF A DATA BREACH

---

- 6.1 On discovery of a data breach, where there has been a loss of **personal data**, the following actions should be taken:
- Control and recovery;
  - Assess the risk;
  - If necessary, notify the Information Commissioner's Office (ICO);
  - Evaluation and response.

## 7.0 CONTROL AND RECOVERY

---

- 7.1 **Who is responsible for action?** The individual committing the breach or their line manager.
- 7.2 The immediate priority is to **contain the breach** and limit its scope and impact.
- 7.3 Where personal data has been sent to someone not authorised to see it staff should:
- tell the recipient not to pass it on or discuss it with anyone else
  - tell the recipient to destroy or delete the personal data they have received and get them to confirm in writing that they have done so
  - warn the recipient of any implications if they further disclose the data
  - inform the data subjects whose personal data is involved what has happened so that they can take any necessary action to protect themselves.
- 7.4 The individual/line manager must immediately report it to the Governance team at [governance@lothian-vjb.gov.uk](mailto:governance@lothian-vjb.gov.uk) providing the following information:
- date and time of the breach
  - date and time breach detected
  - who committed the breach
  - details of the breach
  - number of data subjects involved
  - details of actions already taken in relation to the containment and recovery.

## 8.0 ASSESS THE RISK

---

- 8.1 **Who is responsible for action?** The Data Protection Officer (DPO) or members of the Governance team.

- 8.2 The DPO or a member of the Governance team will conduct an investigation into the breach and prepare a report. This report will follow the [ICO's guidance on Personal data breaches](#) and will consider the following:
- How the breach occurred.
  - The type of personal data involved.
  - Who the data subjects are.
  - The sensitivity of the data breached.
  - What harm to the data subjects can arise? For example, are there risks to physical safety, reputation or financial loss?
  - What could happen if the personal data is used inappropriately or illegally?
  - For personal data that has been lost or stolen, are there any protections in place such as encryption?
  - Are there reputational risks from a loss of public confidence in the service the LVJB provides?

## 9.0 NOTIFYING THE INFORMATION COMMISSIONER

---

- 9.1 **Who is responsible for action?** The DPO or members of the Governance team.
- 9.2 The DPO or members of the Governance team will determine whether the breach is one which is required to be notified to the ICO. A notifiable breach must be reported to the ICO without undue delay, but not later than 72 hours after becoming aware of it.
- 9.3 When reporting a breach, you must provide:
- a description of the nature of the personal data breach including, where possible, the categories and approximate number of individuals concerned;
  - the categories and approximate number of personal data records concerned;
  - the name and contact details of the data protection officer or other contact point where more information can be obtained;
  - a description of the likely consequences of the personal data breach;
  - 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.

## 10.0 EVALUATION AND RESPONSE

---

- 10.1 **Who is responsible for action?** The individual/manager in the area where the breach occurred, DPO and Governance team.
- 10.2 Once the breach has been dealt with the cause of the breach needs to be considered. There may be a need to update policies and procedures, or to conduct additional training.
- 10.3 The DPO and Governance team is responsible for providing guidance and training for LVJB staff on data protection matters and is the central point of contact for LVJB staff on this policy and on all matters relating to the GDPR.