LGSETA
CREATING GREATER IMPACT

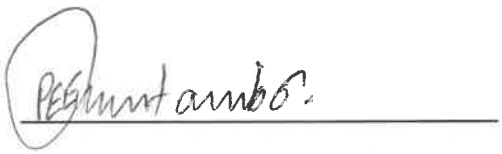
Title:	**Data Breach Policy**	Unique Identifier: **1-09**	
		Document Type: **PL**	
		Revision: **0.1**	
		Total pages:	
		Revision date: **April 2024**	
		Disclosure Classification:	**CONTROLLED DISCLOSURE**

1 DOCUMENT SIGN OFF

AUTHORISED BY

Chief Executive Officer **Date:**

APPROVED BY



Chairperson of the Accounting Authority **Date:**

2.

TABLE OF CONTENTS

3. GLOSSARY OF ABBREVIATIONS AND DEFINITIONS

a. Abbreviations

Abbreviation	Description
CEO	Chief Executive Officer
IFO	Information Commissioner's Office

b. Definitions

Term	Definition
Data	Information in digital form that can be transmitted or processed.
Data Subject	A person to whom personal information relates/ a juristic person i.e., a company.
Personal Data	Any information relating to an individual by which the individual can be identified (directly or indirectly) from that data alone or in combination with other identifiers we possess or can reasonably access.
Data Breach	Any incident, event, or action, whether accidental or deliberate that has the potential to compromise the availability of data, the integrity of data.
Information Regulator	The South African independent body established in terms of section 39 of the Protection of Personal Information Act ,4 of 2013 ("the POPI Act") who is empowered to monitor and enforce compliance with the POPI Act and PAIA Acts.
Information Officer	The CEO of LGSETA is the Information Officer.
Responsible Party	A public or private body or any other person which, alone or in conjunction with others, determines the purpose of and means for processing personal information.

4. DOCUMENT CONTROL

c. Amendment History

Version	Date	Remarks	Name

d. Authorisation

This document has been reviewed and accepted by:

Name	Designation
Ineeleng Molete	Chief Executive Officer (CEO)
Nonhle Mashinini	Acting Chief Operations Officer (COO)
	Chief Financial Officer (CFO)
Jeremiah Thothela	Acting Executive Manager: Corporate Services
Josie Singaram	Acting Executive Manager: Strategy and Planning
	All Managers

e. Document Distribution List

	Designation
Ineeleng Molete	Chief Executive Officer
Nonhle Mashinini	Chief Operations Officer
	Acting Chief Financial Officer
Jeremiah Thothela	Executive Manager: Corporate Services
Josie Singaram	Executive Manager: Strategy and Planning
	All Managers

5. PREAMBLE

The Local Government Sector Education and Training Authority **("LGSETA")** collects and process Personal Information in its daily operations.

Personal data breaches may occur as an error (in operation, or judgement) where the result has been the wrongful disclosure, or loss of private personal data. The primary focus is on personal data, although most of the same considerations apply to other sensitive data, for example containing Accounting Authority sensitive information.

6. PURPOSE AND OBJECTIVE

The purpose of this policy is to provide protection over the processing of data and the information held by the Local Government Sector Education and Training Authority **("LGSETA")**. This policy also outlines the actions that should be taken in the event of a breach to ensure that every care is taken to protect personal data from incidents (accidental or deliberate) to avoid a security breach that could compromise data of the LGSETA.

7. SCOPE

This data breach policy applies to everyone at LGSETA, including employees, temporary or casual staff, consultants, suppliers, service providers, contractors, freelance workers, or other data processors who are storing or processing data on behalf of LGSETA.

7.1 For the purposes of this data breach policy, an incident may include (but is not limited to) any of the following:

7.1.1 Unauthorised use or accessing/modification of data;
7.1.2 Loss or theft of personal or sensitive data;
7.1.3 Loss or theft of equipment on which data has been stored;
7.1.4 Individual error;
7.1.5 Any attempts to gain access to data or LGSETA's IT systems (both successful and failed);
7.1.6 Defacement of web property; and
7.1.7 Physical incidents, like a fire, which could compromise IT systems

7.2. Should LGSETA detect a security breach on any of its systems that contain personal information, LGSETA shall take the required steps to assess the nature and extent of the breach in order to ascertain if any information has been compromised.

7.3 According to Section 22 of the POPI Act, which deals with notification of security compromises, LGSETA must immediately notify stakeholders about unauthorized accesses or acquisitions of personal data.

7.4 LGSETA needs to notify the Information Regulator and the data subject (owner of data) of a security compromise where there are reasonable grounds to believe that the personal information of a data subject had been accessed or acquired by any unauthorised person unless the identity of such data subject cannot be established.

7.5 In terms of section 22 of the POPI Act this notification should include:

7.5.1 The identity of the unauthorised person, if known, who accessed or acquired the personal information;
7.5.2 A description of the possible consequences of the security compromise;
7.5.3 A description of the measures taken or proposed to be taken by the responsible party to remedy the security breach; and
7.5.4 A recommendation of the measures to be taken from any party whose personal information was leaked in the security breach.

7.6 LGSETA shall notify the affected parties should it have reason to believe that their information has been compromised. Such notification shall only be made where LGSETA can identify the data subject to which the information relates. Where it is not possible it may be necessary to consider website publication and whatever else the Information Regulator prescribes.

7.7 Notification will be provided in writing by means of either:

7.7.1 Email; or

7.7.2 Registered mail; or

7.7.3 Placed on website.

7.8 The notification shall provide the following information where possible:

7.8.1 Description of possible consequences of the breach;

7.8.2 Measures taken to address the breach;

7.8.3 Recommendations to be taken by the data subject to mitigate adverse effects; and

7.8.4 The identity of the party responsible for the breach.

7.9 All employees who access, manage, or use data in any way are responsible for reporting a data breach or any other type of security incident. The POPI Act clearly states that an exception to a breach notification is if the identity of data subjects cannot be established.

7.10 Any person who provides false information, or tries to hinder, obstruct, or unlawfully influence the Information Regulator on any matter, will be held liable to a fine or imprisonment. Should LGSETA detect a security breach on any of its systems that contain personal information, LGSETA shall take the required steps to assess the nature and extent of the breach to ascertain if any information has been compromised.

8. POLICY PROVISIONS

8.1 Procedure

On discovery of a data breach the following actions should be taken:

8.2 Containment and recovery

8.2.1 In the event of a data breach, steps to ensure containment should immediately be actioned by limiting further access to the affected personal information, or the possible compromise of other information.

8.2.2 The individual committing the breach or having identified a possible breach should immediately inform their Manager or the Information Officer.

8.2.3 In order to determine the appropriate response, the following questions should be considered:

8.2.4 How did the data breach occur?

8.2.5 Is the personal information still being shared, disclosed, or lost without authorisation?

8.2.6 Who has access to the personal information?

8.2.7 What can be done to secure the information, or stop the unauthorised access or disclosure, and reduce the risk of harm to affected individuals?

8.3 Assessing the risk

8.3.1 An assessment of the data breach will help LGSETA to understand the risks posed by the data breach and how these risks can be addressed, this should be done as soon as practically possible.

8.3.2 The assessment is used to establish the severity of the incident. The initial assessment should also include analysing whether there is any way to recover the lost data, and mitigate further risks associated with the incident.

8.3.3 The Information Officer or a nominated person will investigate the breach and prepare a Breach Report within 72 hours.

8.3.4 The assessment of the data breach will guide the decision on whether to notify affected individuals.

8.3.5 In the assessment of a data breach, it is important to consider:

8.3.6 the type or types of personal information involved in the data breach;

8.3.7 the circumstances of the data breach, including its cause and extent; and

8.3.8 the nature of the harm to affected individuals, and if this harm can be removed through remedial action.

8.4 Notification of breach to the Information Commissioner's Office (ICO)

8.4.1 Under the POPI Act, where there are reasonable grounds to believe that a data subject's personal information has been accessed or acquired by an unauthorised person, the responsible party, or any third-party processing personal information under the authority of the responsible party, must notify the Information Regulator and the data subject thereof, unless the identity of the data subject cannot be established.

8.4.2 Notification to the data subject must be:

8.4.2.1 made as soon as reasonably possible after the discovery of the breach;

8.4.2.2 sufficiently detailed; and

8.4.2.3 in writing and communicated to the data subject by mail (to the data subject's last known physical or postal address), email to the data subject's last known email address, placement in a prominent position on the website of the responsible party, publication in the news media, or as may be directed by the Information Regulator.

8.4.3 The notification to a data subject must be in writing and communicated to the data subject in at least one of the following ways:

8.4.3.1 Mailed to the data subject's last known physical or postal address;
8.4.3.2 sent by e-mail to the data subject's last known e-mail address;
8.4.3.3 placed in a prominent position on the website of the responsible party; and
8.4.3.4 published in the news media; or as may be directed by the Regulator.
8.4.3.5 The notification should provide the data subject with sufficient detail in order to allow the data subject to take the appropriate protective measures;
8.4.3.6 A responsible party may be directed by the Information Regulator to publicise the breach where the Information Regulator has reasonable grounds to believe that such publicity would protect the data subject; and
8.4.3.7 Depending on the exact case, the notification would have to be either physically or electronically mailed to the data subject, published on the organisation's website, or announced to the media.

8.5 Evaluation and response

8.5.1 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.

8.5.2 It is also important to conduct an extensive review detailing:
8.5.2.1. The cause of the breach;
8.5.2.2. The effectiveness of any response; and
8.5.2.3 Whether any changes to existing ICT systems, company procedures or policies must be implemented

PEE

9 LEGAL & REGULATORY OBLIGATIONS

The following legislation is applicable to this policy:

9.1. The Protection of Personal Information Act (2013) ("POPIA");

9.2. Promotion of Access to Information Act (2000) ("PAIA"); and

9.3. Electronic Communications and Transactions Act, 2002 ("ECTA").

10 REVIEW PROCESS

The Data Breach Policy shall be reviewed and updated in two years and/or as and when necessary changes in the applicable legislation or business imperatives occur.