

Data Security Policy

Introduction

OpenEMIS collects and uses information about individuals in order to strengthen education planning and monitoring. These data may include information about students, guardians, staff and other people in the community. This policy describes how OpenEMIS ensures that this personal data is collected, handled and stored in full compliance with data protection standards.

Why this policy exists

This data protection policy ensures OpenEMIS:

- Complies with data protection law and follows good practices
- Protects the rights of students, guardians, staff and the community
- Is transparent about how the system stores and processes individuals' data
- Protects itself from the risks of a data breach

Data protection law

Most countries have data security policies that describe how personal information on individuals are to be collected, managed, stored, and distributed.

These policies apply regardless of whether data is stored electronically, on paper or on other media.

To comply with the laws that support these policies, personal information must be collected and used fairly, stored safely, and not disclosed unlawfully.

These laws are generally underpinned by eight important principles that state that personal information is to:

1. Be processed fairly and lawfully;
2. Be obtained only for specific, lawful purposes;
3. Be adequate, relevant and not excessive;
4. Be accurate and kept up to date;
5. Not be held for any longer than necessary;
6. Be processed in accordance with the rights of data subjects;
7. Be protected in appropriate ways;
8. Not be transferred to another territory without adequate levels of protection.

People, risks and responsibilities

Policy scope

This policy applies to:

- All authorised users involved in the OpenEMIS initiative;
- All staff, contractors, volunteers and other people working on behalf of OpenEMIS.

It applies to all data that OpenEMIS holds relating to identifiable individuals. This can include:

- Names of individuals;
- Contact information such as addresses, phone and email;
- Identity information;
- Health information;
- Academic information;
- ...plus any other information relating to individuals

Data protection risks

This policy helps to protect OpenEMIS from some data security risks, including:

- **Breaches of confidentiality.** For instance, information being given out inappropriately.
- **Failing to offer choice.** For instance, all individuals should be free to choose how the data are used relating to them.
- **Reputational damage.** For instance, OpenEMIS could suffer if hackers successfully gained access to sensitive data.

Responsibilities

Everyone who works for or with OpenEMIS has responsibility for ensuring data are collected, stored and handled appropriately. Each team that handles personal data must comply with these policy and data protection principles.

Furthermore, people with these OpenEMIS roles have key areas of responsibility:

- The **OpenEMIS Steering Committee** is ultimately responsible for ensuring that OpenEMIS meets its data security legal obligations.
- The **OpenEMIS Data Security Officer** is responsible for:
 - Keeping the OpenEMIS initiative updated about data protection responsibilities, risks and issues;
 - Reviewing all data protection procedures and related policies, in line with an agreed schedule;
 - Arranging data protection training and advice for the people covered by this policy;
 - Handling data protection questions from staff and anyone else covered by this policy;
 - Responding to requests from individuals to see the data OpenEMIS holds about them (also called 'subject access requests');

- Checking and approving any contracts or agreements with third parties that may handle OpenEMIS data.
- The **OpenEMIS IT Director**, is responsible for:
 - Ensuring all systems, services and equipment used for storing data meet acceptable security standards;
 - Performing regular checks and scans to ensure security hardware and software is functioning properly;
 - Evaluating the data security compliance of any third-party services that OpenEMIS may use to store or process data, such as, cloud computing services;
 - Approving any data protection statements attached to communications, such as, emails and letters;
 - Addressing any data protection queries from journalists or media outlets, like newspapers;
 - Where necessary, working with other staff to ensure marketing initiatives abide by data protection principles.

General guidelines

- The only people authorised to access data covered by this policy are those who **need the data to carry out their official OpenEMIS responsibilities**.
- Data **should not be shared informally**. When access to confidential information is required, authorized users must request approval in writing from their line managers.
- All people handling OpenEMIS data need to understand their responsibilities when handling the data.
- All people authorised to access OpenEMIS data must ensure that all data are secure, by taking appropriate precautions and following the guidelines herein:
 - In particular, **strong passwords must be used** and should never be shared.
 - Personal data **should not be disclosed** to unauthorised people, either within the OpenEMIS team or externally.
 - Data should be **regularly reviewed and updated** if out of date. If no longer required, the data should be deleted and disposed of.
 - Anyone using OpenEMIS data **should request help** from their line manager if they are unsure about any aspect of data security and protection.

Data access

This policy provides guidance on who, how and what type of data should be accessed:

- The only people authorised to access OpenEMIS data covered by this policy are those who require the data to carry out their **approved roles and responsibilities**;

- OpenEMIS data always remains the property of the client and is not authorised for use for any reason without the written consent of the client;
- Access to OpenEMIS data is only allowed via approved APIs. Direct access to OpenEMIS databases is only authorised to system administrators with the approved roles and responsibilities for managing the backend of the system.

Data storage

These rules describe how and where data must be safely stored. Questions about storing data safely should be directed to the IT director.

When data is stored on paper, it should be kept in a secure place where unauthorised people cannot see it. These guidelines also apply to data that are usually stored electronically but have been printed out for any reason.

- When not required, the paper or files should be kept **in a locked drawer or filing cabinet**.
- Employees should make sure paper and printouts are **not left where unauthorised people could see them**, like on a printer.
- **Data printouts should be shredded** and disposed of securely when no longer required.

When data is **stored electronically**, it must be protected from unauthorised access, accidental deletion and malicious hacking attempts:

- Data should be **protected by strong passwords** that are changed regularly and never shared with others.
- If data is **stored on removable media** (like a CD-ROM or USB drive), these should be kept locked away securely when not being used.
- Data should only be stored on **designated drives and servers**, and should only be uploaded on **approved cloud computing services**.
- Servers containing personal data should be **situated in a secure location**, away from general office space.
- Data should be **backed up frequently and securely stored**. These backups should be tested regularly, in line with the OpenEMIS standard backup procedures.
- Data should **never be saved directly** to laptops or other mobile devices like tablets or smart phones.
- All servers and computers containing data should be protected by **approved security software and a firewall**.

Data use

There is a significant data security risk when OpenEMIS data are accessed and used. During this time, there is the greatest risk of loss, corruption or theft:

- When working with personal data, authorised users should ensure **the screens of their computers are always locked** when left unattended;
- Personal data **should not be shared informally**. In particular, it should never be sent by email, as this form of communication is not secure;
- Data must be **encrypted before being transferred electronically**; the IT director can explain how to send data to authorised external contacts;
- Authorised users **should not save copies of OpenEMIS data to their own computers**; – always access and update the centralised instance of the database.

Data accuracy

The OpenEMIS initiative takes reasonable steps to ensure data is kept accurate and up-to-date.

- Data is stored in **as few places as necessary** and authorised users do not create any unnecessary additional data sets;
- Data is **updated as inaccuracies are discovered**, and, if no longer required, the data will be removed from the database.

Subject access requests

All individuals who are the subject of personal data held by OpenEMIS are entitled to:

- Ask **what information** OpenEMIS holds about them and why;
- Ask **how to gain access** to it;
- Be informed **how to keep it up-to-date**;
- Be informed how OpenEMIS is **meeting its data protection obligations**.

If an individual contacts OpenEMIS requesting this information, this is called a subject access request. These requests must be made in writing. The identity of anyone making a subject access request will need to be verified and approved before providing any information.

Disclosing data for other reasons

In certain circumstances, laws allow OpenEMIS data to be disclosed to law enforcement agencies without the consent of the data subject. Under these circumstances, OpenEMIS will disclose requested data. However, the OpenEMIS team will ensure the request is legitimate, seeking assistance from management and legal advisers when necessary.

Providing information

The OpenEMIS initiative aims to ensure that individuals are aware how their personal data are being processed, and that they understand:

- How the data is being used;
- How to exercise their rights.