SIMS helping schools inspire

Accredited Support

Keystone MIS

SIMS Support & Training

General Data Protection Regulation Policy

Service Desk: 01482 238 700
Email: Support@KeystoneMIS.co.uk

www.KeystoneMIS.co.uk

https://tinyurl.com/Support-SIMS

Context and Overview

Key details

Introduction

Keystone MIS needs to gather and use certain information about individuals and schools.

These can include customers, suppliers, business contacts, employees and other people the organisation has a relationship with or may need to contact.

This policy describes how this personal data must be collected, handled and stored to meet the company's data protection standards — and to comply with the law.

Why this policy exists

This data protection policy ensures Keystone MIS:

- Complies with data protection law and follows good practice.
- Protects the rights of staff, customers and partners.
- Is open about how it stores and processes individuals' data.
- Protects itself from the risks of a data breach.

Data protection law

The General Data Protection Regulation describes how organisations — including Keystone MIS — must collect, handle and store personal information.

These rules apply regardless of whether data is stored electronically, on paper or on other materials.

To comply with the law, personal information must be collected and used fairly, stored safely and not disclosed unlawfully.

GDPR is underpinned by six privacy principles. Keystone MIS shall comply with the principles of data protection (the principles) enumerated in the EU General Data Protection Regulation. We will make every effort possible in everything we do to comply with these principles. The Principles are:

1. Lawfulness, fairness and transparency
2. Purpose Limitations
3. Data Minimisation
4. Accuracy
5. Storage Limitations
6. Integrity and Confidentiality

People, Risks and Responsibilities

Policy scope

This policy applies to:

- The company offices of Keystone MIS.
- All staff of Keystone MIS.
- All contractors, suppliers and other people working on behalf of Keystone MIS.

It applies to all data that the company holds relating to identifiable individuals, even if that information technically falls outside of the GDPR. This can include:

- Names of individuals
- Postal addresses
- Email addresses
- Telephone numbers

Data protection risks

This policy helps to protect Keystone MIS from some very real 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 company uses data relating to them.
- Reputational damage. For instance, the company could suffer if hackers successfully gained access to sensitive data.

Responsibilities

Everyone who works for or with Keystone MIS has some responsibility for ensuring data is collected, stored and handled appropriately.

Each person that handles personal data must ensure that it is handled and processed in line with this policy and data protection principles.

However, these people have key areas of responsibility:

The board of directors is ultimately responsible for ensuring that Keystone MIS meets its legal obligations.

The data protection officer, Richard Morrell, is responsible for:

- o Keeping the board updated about data protection responsibilities, risks and issues.
- o Reviewing all data protection procedures and related policies, in line with an agreed schedule.
- o Arranging data protection training and advice forthe people covered by this policy.
- o Handling data protection questions from staff and anyone else covered by this policy.
- o Dealing with requests from individuals to see the data Keystone MIS holds about them (also called 'subject access requests').
- o Checking and approving any contracts or agreements with third parties that may handle the company's sensitive data.
- o Ensuring all systems, services and equipment used for storing data meet acceptable security standards.
- o Performing regular checks and scans to ensure security hardware and software is functioning properly.
- o Evaluating any third-party services the company is considering using to store or process data. For instance, cloud computing services.
- o Approving any data protection statements attached to communications such as emails and letters.
- o Addressing any data protection queries from journalists or media outlets like newspapers.
- o Where necessary, working with other staff to ensure marketing initiatives abide by data protection principles

General Staff Guidelines

The only people able to access data covered by this policy should be those who need it for their work.

Data should not be shared informally.

Employees should keep all data secure, by taking sensible precautions and following the guidelines below.

In particular, strong passwords must be used and they should never be shared.

Personal data should not be disclosed to unauthorised people, either within the company or externally.

Data should be regularly reviewed and updated if it is found to be out of date. If no longer required, it should be deleted and disposed of.

Employees should request help from their line manager or the data protection officer if they are unsure about any aspect of data protection.

Data Storage

These rules describe how and where data should be safely stored. Questions about storing data safely can be directed to the data controller.

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 is usually stored electronically but has been printed out for some 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 between employees.
- If data is stored on removable media (like a CD or DVD), 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 CAPITA when requested with the required encryption.
- Servers containing personal data should be sited in a secure location, away from general office space.
- Data should be backed up frequently. Those backups should be tested regularly, in line with the company's 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

Personal data is of no value to Keystone MIS unless the business can make use of it. However, it is when personal data is accessed and used that it can be at the greatest risk of loss, corruption or theft:

- When working with personal data, employees 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. Pupil data in particular should never be shared in an unsecured format.
- Data must be encrypted before being transferred electronically. The Data Protection Officer can explain how to send data to authorised external contacts.
- Employees should not save copies of personal data to their own computers.
- Always access and update the central copy of any data.
- All data that is to be stored or used to resolve a customer case will be sent to CAPITA under their guidelines and destroyed by Keystone MIS on the resolution of the case.
- CAPITA Data Use policies can be found on the Support Site here: http://bit.ly/gdprcapita

Data Accuracy

The law requires Keystone MIS to take reasonable steps to ensure data is kept accurate and up todate.

The more important it is that the personal data is accurate, the greater the effort Keystone MIS should put into ensuring its accuracy.

It is the responsibility of all employees who work with data to take reasonable steps to ensure it is kept as accurate and up to date as possible.

- Data will be held in as few places as necessary. Staff should not create any unnecessary additional data sets.
- Staff should take every opportunity to ensure data is updated. For instance, by confirming a customer's details when they call.
- Data should be updated as inaccuracies are discovered. For instance, if a customer can no longer be reached on their stored telephone number, it should be removed from the database.

Subject Access Requests

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

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

If an individual contacts the company requesting this information, this is called a subject access request. Subject access requests from individuals should be made by email, addressed to the data controller at Richard.Morrell@keystonemis.co.uk. The data controller can supply a standard request form, although individuals do not have to use this.

The data controller will aim to provide the relevant data within 14 days.

The data controller will always verify the identity of anyone making a subject access request before handing over any information.