

SIGTA Data Protection Policy

Introduction

SIGTA Ltd. needs to keep certain personal information (referred to in the General Data Protection Regulations (GDPR) as personal data), for example about its staff and learners, to fulfil its stated objectives and to meet its legal obligations to funding bodies and the government. To comply with the law, information must be collected and used fairly, stored safely and not disclosed to any other person unlawfully. To do this, SIGTA must meet its obligations under the GDPR and comply with the Data Protection Principles which are set out in the Data Protection Act, 2018.

Principles

Personal data shall:

- Be obtained and processed fairly and lawfully and shall not be processed unless certain conditions are met.
- Be obtained for a specified and lawful purpose and shall not be processed in any manner incompatible with that purpose.
- Be adequate, relevant and not excessive for those purposes.
- Be accurate and kept up to date.
- Not be kept for longer than is necessary for that purpose.
- Be processed in accordance with the data subject's rights.
- Be kept secure from unauthorised access, accidental loss or destruction.
- Not be transferred to a country outside the European Economic Area, unless that country has equivalent levels of protection for personal data.

SIGTA and its staff who process or use personal information must ensure that they follow these principles at all times. In order to ensure that this happens, SIGTA has developed this Data Protection Policy.

Status of the Policy

This policy has been approved by SIGTA and any breach will be taken seriously and may result in formal action.

Any member of staff or a learner who considers that the policy has not been followed in respect of personal data about themselves should raise the matter with the CEO.

Notification of Data Held and Processed

All staff, learners and other users are entitled to:

- Ask what information SIGTA holds about them and why.
- Ask how to gain access to it.
- Be informed how to keep it up to date.
- Be informed what SIGTA is doing to comply with its obligations under the GDPR and Data Protection Act 2018.



Responsibilities of Staff and Learners

All staff and learners are responsible for:

- Checking that any personal data that they provide to SIGTA is accurate and up to date.
- Informing SIGTA of any changes to information which they have provided, e.g. changes of address.
- Checking the accuracy of any information that SIGTA may send out from time to time.
- Staff to provide details of information that is being kept and processed.

If, as part of their responsibilities, staff collect information about other people (e.g. about learners work or personal circumstances), they must comply with this Policy.

Data Security

The need to ensure that data is kept securely means that precautions must be taken against physical loss or damage, and that both access and disclosure must be restricted. All staff are responsible for ensuring that:

- Any personal data which they hold is kept securely
- Personal information is not disclosed either orally or in writing or otherwise to any unauthorised third party.

Rights to Access Information

Staff and learners and other users of SIGTA have the right to access any personal data that is being kept about them on computer and also have access to paper-based data held in certain manual filing systems. Any person who wishes to exercise this right should make a request in writing to the SIGTA Company Secretary or CEO.

SIGTA will comply with requests for access to personal information as quickly as possible and will aim to ensure information is provided within 30 days of an accepted request. In exceptional circumstances if this is not possible, the reason for delay will be explained in writing to the individual making the request.

Publication of SIGTA Information

Information that is already legitimately in the public domain is exempt from the Data Protection Act 2018.

Subject Consent

The need to process data for legitimate purposes has been communicated to staff, and to learners at enrolment. In some cases, if the data is sensitive, for example information about health, race or gender, express consent to process the data must be obtained. Processing may be necessary to operate SIGTA policies, such as health and safety and equal opportunities.



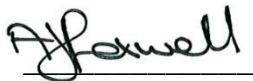
Retention of Data

SIGTA will keep some forms of information for longer than others to ensure the objectives for holding the data are fully met. Personal data relating to SIGTA learners will not be held for longer than required to fulfil SIGTA's legitimate objectives and to meet the compliance requirements of funding authorities and other approved third party bodies.

SIGTA's Designated Data Controller

SIGTA is the data controller under the Act and is therefore ultimately responsible for implementation. Day to day matters will be dealt with by the CEO. Any questions or concerns about the interpretation or operation of this policy should be taken up with the CEO.

Approved:



Name: Alison Foxwell

Position: CEO

Date: October 2023 - Version 1.6

Reviewed: Oct 2023

Next review due: Oct 2024.

