# SIGTA LTD

## DATA Protection Policy

## Including GDPR

| Date | Version | Description | Checked | Approved |
|---|---|---|---|---|
| 15-01-26 | 1.8 | Annual review of this policy review completed.<br><br>Minor updates to format and content (format).<br><br>Introduction of version control table to record amendments made. |  <br><br>Mike Driscoll<br><br>IQA - SIGTA |  <br><br>Alison Foxwell<br><br>CEO -SIGTA |

***Next revision due: 15-01-27***

## 1. Introduction

SIGTA Ltd (hereinafter referred to as "the Provider") is committed to ensuring the security and protection of the personal data that we process, and to providing a compliant and consistent approach to data protection. This policy outlines our commitment to GDPR (General Data Protection Regulation) compliance, ensuring that personal data is handled appropriately and securely.

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.

## 2. Purpose

The purpose of this policy is to:

- Comply with data protection law and follow good practice.
- Protect the rights of employees, apprentices, and stakeholders.
- Ensure transparency about how personal data is collected, stored, and processed.
- Protect the Provider from the risks of data breaches and other data-related incidents.

## 3. Scope

This policy applies to all employees, apprentices, contractors, and stakeholders of the Provider who have access to or process personal data. It covers all personal data that the Provider processes regardless of the format or media on which it is stored.

## 4. Definitions

**Personal Data:** Any information relating to an identified or identifiable natural person.

**Data Subject:** The identified or identifiable person to whom the personal data relates.

**Processing:** Any operation performed on personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation, alteration, retrieval, consultation, use, disclosure, dissemination, alignment, combination, restriction, erasure, or destruction.

**Data Controller:** The entity that determines the purposes and means of processing personal data.

**Data Processor:** The entity that processes personal data on behalf of the Data Controller.

## 5. Principles

The Provider adheres to the principles relating to the processing of personal data set out in the GDPR. These principles require that personal data shall be:

1. **Processed lawfully, fairly, and in a transparent manner.**
2. **Collected for specified, explicit, and legitimate purposes and not further processed in a manner that is incompatible with those purposes.**
3. **Adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed.**
4. **Accurate and, where necessary, kept up to date.**
5. **Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.**

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.

SIGTA and its staff who process or use personal information must ensure that they follow these principles at all times.

## 6. Lawful Basis for Processing

The Provider will only process personal data where it has a lawful basis for doing so. The lawful bases for processing are:

- **Consent:** The data subject has given clear consent for the processing of their personal data for a specific purpose.
- **Contract:** The processing is necessary for a contract the Provider has with the data subject, or because they have asked the Provider to take specific steps before entering into a contract.
- **Legal Obligation:** The processing is necessary for the Provider to comply with the law.
- **Vital Interests:** The processing is necessary to protect someone's life.
- **Public Task:** The processing is necessary for the Provider to perform a task in the public interest or for its official functions.
- **Legitimate Interests:** The processing is necessary for the Provider's legitimate interests or the legitimate interests of a third party, unless there is a good reason to protect the individual's personal data which overrides those legitimate interests.

### 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.

## 7. Data Subject Rights

Data subjects have the following rights regarding their personal data:

- **Right to be Informed:** Individuals have the right to be informed about the collection and use of their personal data.
- **Right of Access:** Individuals have the right to access their personal data and supplementary information.
- **Right to Rectification:** Individuals have the right to have inaccurate personal data rectified, or completed if it is incomplete.
- **Right to Erasure:** Individuals have the right to have personal data erased in certain circumstances.
- **Right to Restrict Processing:** Individuals have the right to request the restriction or suppression of their personal data in certain circumstances.
- **Right to Data Portability:** Individuals have the right to obtain and reuse their personal data for their own purposes across different services.
- **Right to Object:** Individuals have the right to object to the processing of their personal data in certain circumstances.
- **Rights Related to Automated Decision-Making and Profiling:** Individuals have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning them or similarly significantly affects them.

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.

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.

**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.
- 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.

## 8. Data Security

The Provider will ensure that data is kept securely and precautions are 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.
- Ongoing confidentiality, integrity, availability, and resilience of processing systems and services

## 9. Data Breaches

In the event of a data breach, the Provider will:

- Notify the Information Commissioner's Office (ICO) within 72 hours of becoming aware of the breach, where feasible.
- Inform affected individuals without undue delay if the breach is likely to result in a high risk to their rights and freedoms.
- Document all data breaches, including the facts relating to the breach, its effects, and the remedial action taken.

Any data 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.

## 10. 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.

## 11. Third-Party Processors

The Provider will ensure that any third-party processors are compliant with GDPR and have appropriate measures in place to protect personal data. Contracts with third-party processors will include specific terms to ensure compliance with GDPR requirements.

## 12. Training and Awareness

SIGTA will provide GDPR training to all employees and apprentices to ensure they understand their responsibilities under GDPR and this policy. Regular updates and refresher training will be provided as necessary.

## 13. Review of Policy

This Data Protection and GDPR Policy will be reviewed annually or as needed to ensure its effectiveness and compliance with legal requirements.

## 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.

## 14. Contact Information

For any questions or further information regarding this policy, please contact:

**Data Protection Officer (DPO) Contact Information:**

Email: afoxwell@sigta.co.uk

Telephone: 01273 416989/ 07793 269615

By implementing and enforcing this policy, the Provider demonstrates its commitment to protecting personal data and ensuring GDPR compliance.