



# **SWAAT Quality Policy**

Data Protection Policy





## Table of Contents

<b>1</b>	<b>INTRODUCTION</b> .....	<b>4</b>
<b>2</b>	<b>REFERENCES</b> .....	<b>4</b>
<b>3</b>	<b>DEFINITIONS</b> .....	<b>4</b>
<b>4</b>	<b>ABOUT OUR ORGANISATION</b> .....	<b>ERROR! BOOKMARK NOT DEFINED.</b>
4.1	ORGANISATIONAL CONTEXT.....	4
4.2	RELEVANT INTERESTED PARTIES.....	5
4.3	QUALITY MANAGEMENT SYSTEM.....	<b>ERROR! BOOKMARK NOT DEFINED.</b>
4.3.1	Management System Scope.....	<b>Error! Bookmark not defined.</b>
4.3.2	Management System Processes .....	<b>Error! Bookmark not defined.</b>
4.3.3	Outsourced Processes .....	<b>Error! Bookmark not defined.</b>
4.3.4	Documented Information.....	<b>Error! Bookmark not defined.</b>
<b>5</b>	<b>LEADERSHIP AND GOVERNANCE</b> .....	<b>ERROR! BOOKMARK NOT DEFINED.</b>
5.1	LEADERSHIP AND COMMITMENT.....	<b>ERROR! BOOKMARK NOT DEFINED.</b>
5.1.1	Quality Management .....	<b>Error! Bookmark not defined.</b>
5.1.2	Customer Focus .....	<b>Error! Bookmark not defined.</b>
5.1.3	Quality Policy .....	<b>Error! Bookmark not defined.</b>
5.2	ROLE, RESPONSIBILITIES AND AUTHORITIES .....	<b>ERROR! BOOKMARK NOT DEFINED.</b>
5.3	COMMUNICATION .....	<b>ERROR! BOOKMARK NOT DEFINED.</b>
5.3.1	Internal Communication .....	<b>Error! Bookmark not defined.</b>
5.3.2	External Communication .....	<b>Error! Bookmark not defined.</b>
<b>6</b>	<b>MANAGEMENT SYSTEM PLANNING</b> .....	<b>ERROR! BOOKMARK NOT DEFINED.</b>
6.1	ADDRESSING RISKS AND OPPORTUNITIES .....	<b>ERROR! BOOKMARK NOT DEFINED.</b>
6.2	QUALITY OBJECTIVES.....	<b>ERROR! BOOKMARK NOT DEFINED.</b>
6.3	PLANNING FOR CHANGE.....	<b>ERROR! BOOKMARK NOT DEFINED.</b>
<b>7</b>	<b>SUPPORT</b> .....	<b>ERROR! BOOKMARK NOT DEFINED.</b>
7.1	RESOURCES.....	<b>ERROR! BOOKMARK NOT DEFINED.</b>
7.1.1	General.....	<b>Error! Bookmark not defined.</b>
7.1.2	People.....	<b>Error! Bookmark not defined.</b>
7.1.3	Infrastructure.....	<b>Error! Bookmark not defined.</b>
7.1.4	Operational Environment.....	<b>Error! Bookmark not defined.</b>
7.1.5	Monitoring and Measurement Tools .....	<b>Error! Bookmark not defined.</b>
7.1.6	Organisational Knowledge.....	<b>Error! Bookmark not defined.</b>
<b>8</b>	<b>PRODUCT AND SERVICE DEVELOPMENT</b> .....	<b>ERROR! BOOKMARK NOT DEFINED.</b>
8.1	OPERATIONAL PLANNING AND CONTROL.....	<b>ERROR! BOOKMARK NOT DEFINED.</b>
8.2	CUSTOMER REQUIREMENTS.....	<b>ERROR! BOOKMARK NOT DEFINED.</b>
8.2.1	Customer Communication .....	<b>Error! Bookmark not defined.</b>
8.2.2	Determining Requirements .....	<b>Error! Bookmark not defined.</b>
8.2.3	Review of Requirements .....	<b>Error! Bookmark not defined.</b>
8.2.4	Changes in Requirements .....	<b>Error! Bookmark not defined.</b>
8.3	DESIGN AND DEVELOPMENT .....	<b>ERROR! BOOKMARK NOT DEFINED.</b>
8.3.1	General .....	<b>Error! Bookmark not defined.</b>

8.3.2	Planning.....	<b>Error! Bookmark not defined.</b>
8.3.3	Inputs.....	<b>Error! Bookmark not defined.</b>
8.3.4	Controls.....	<b>Error! Bookmark not defined.</b>
8.3.5	Outputs.....	<b>Error! Bookmark not defined.</b>
8.3.6	Changes.....	<b>Error! Bookmark not defined.</b>
8.4	CONTROL OF SUPPLIERS AND EXTERNAL PROCESSES.....	<b>ERROR! BOOKMARK NOT DEFINED.</b>
8.4.1	General.....	<b>Error! Bookmark not defined.</b>
8.4.2	Purchasing Controls.....	<b>Error! Bookmark not defined.</b>
8.4.3	Purchasing Information.....	<b>Error! Bookmark not defined.</b>
8.5	PRODUCTION AND SERVICE PROVISION.....	<b>ERROR! BOOKMARK NOT DEFINED.</b>
8.5.1	Control of Production and Service Provision.....	<b>Error! Bookmark not defined.</b>
8.5.2	Identification and Traceability.....	<b>Error! Bookmark not defined.</b>
8.5.3	3 <sup>rd</sup> Party Property.....	<b>Error! Bookmark not defined.</b>
8.5.4	Preservation.....	<b>Error! Bookmark not defined.</b>
8.5.5	Post-delivery Activities.....	<b>Error! Bookmark not defined.</b>
8.5.6	Control of Changes.....	<b>Error! Bookmark not defined.</b>
8.6	RELEASE OF PRODUCTS AND SERVICES.....	<b>ERROR! BOOKMARK NOT DEFINED.</b>
8.7	CONTROL OF NON-CONFORMING OUTPUTS.....	<b>ERROR! BOOKMARK NOT DEFINED.</b>
<b>9</b>	<b>PERFORMANCE EVALUATION.....</b>	<b>ERROR! BOOKMARK NOT DEFINED.</b>
9.1	MONITORING, MEASUREMENT, ANALYSIS AND EVALUATION.....	<b>ERROR! BOOKMARK NOT DEFINED.</b>
9.1.1	General.....	<b>Error! Bookmark not defined.</b>
9.1.2	Customer Satisfaction.....	<b>Error! Bookmark not defined.</b>
9.1.3	Analysis and Evaluation.....	<b>Error! Bookmark not defined.</b>
9.2	INTERNAL AUDIT.....	<b>ERROR! BOOKMARK NOT DEFINED.</b>
9.3	MANAGEMENT REVIEW.....	<b>ERROR! BOOKMARK NOT DEFINED.</b>
9.3.1	General.....	<b>Error! Bookmark not defined.</b>
9.3.2	Inputs.....	<b>Error! Bookmark not defined.</b>
9.3.3	Outputs.....	<b>Error! Bookmark not defined.</b>
<b>10</b>	<b>IMPROVEMENT.....</b>	<b>ERROR! BOOKMARK NOT DEFINED.</b>
10.1	GENERAL.....	<b>ERROR! BOOKMARK NOT DEFINED.</b>
10.2	NON-CONFORMITY AND CORRECTIVE ACTION.....	<b>ERROR! BOOKMARK NOT DEFINED.</b>
10.3	IMPROVEMENT.....	<b>ERROR! BOOKMARK NOT DEFINED.</b>
<b>APPENDICES.....</b>		<b>ERROR! BOOKMARK NOT DEFINED.</b>
A.1	CORRELATION MATRIX.....	<b>ERROR! BOOKMARK NOT DEFINED.</b>
A.2	SEQUENCE AND INTERACTION OF PROCESSES.....	<b>ERROR! BOOKMARK NOT DEFINED.</b>
A.3	ORGANISATION CHART.....	<b>ERROR! BOOKMARK NOT DEFINED.</b>

## 1 Introduction

South West Assessment and Training (SWAAT) needs to gather and use certain information about individuals. These can include customers, suppliers, business contacts, employees and other people who the organization has a relationship with or may need to contact.

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

## 2 References

In addition to ISO 9001:2015 we also make reference to other relevant British and/or international standards as well as customer specifications appropriate to our products and market.

Standard	Title	Description
The EU General Data Protection Regulation (GDPR) 2018	Data Protection Act	Deals with data protection in the UK

## 3 Why this policy exists

This data protection policy ensures SWAAT:

1. Complies with data protection law and follows good practices.
2. Protects the rights of our staff, customers and anyone we have a professional relationship with.
3. Is open about how it stores and processes individuals' data.
4. Protects itself from the risks of a data breach.

## 4 Data Protection Law

### 4.1 Context

The Data Protection Act, 1998, describes how organisations, including SWAAT, must collect, handle and store personal information.

These rules apply regardless of whether data is stored electronically, on paper or on tablets of stone.

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

The Data Protection Act is underpinned by eight important principles. These state personal data must:

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. Processed in accordance with the rights of data subjects
7. Be protected in appropriate ways
8. Not be transferred outside of the European Economic Area (EEA), unless that country or territory also ensures an adequate level of protection.

## 4.2 Policy Scope

The policy applies to:

- SWAAT's office in Liskeard;
- All staff of SWAAT
- All suppliers

It applies to all data that the company holds relating to identifiable individuals, even if that information technically falls outside of the Data Protection Act, 1998. This includes:

- Names of individuals
- Postal addresses
- Email addresses
- Telephone numbers
- NI numbers
- Qualifications undertaken

## 4.3 Data Protection Risks

This policy helps to protect SWAAT 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 SWAAT uses the data that relates to them.
- Reputational damage: For instance, SWAAT could suffer if hackers successfully gained access to sensitive data.

### 4.3.1 Responsibilities

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

Each individual who 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 management team are ultimately responsible to ensure that SWAAT meets its legal obligations.
- Kevin Kendall, the data protection officer, is responsible for:
  - Keeping everyone 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 people covered by this policy.
- Handling data protection questions from staff and anyone else covered by this policy.
- Dealing with requests from individuals to see the data that SWAAT holds about them (also called 'subject access requests').
- Ensuring all systems, services and equipment used for storing data meet acceptable security standards.
- Performing checks and scans to ensure hardware and software is performing and functioning properly.
- Evaluating any third-party services the company is considering using to store or process data. For instance, cloud storage.
- Approving any data protection statements attached to communications such as emails and letters.
- Where necessary, like never, addressing any data protection queries from any media outlets.
- Where necessary, working with staff to ensure marketing initiatives abide by the data protection principles.

#### 4.3.2 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. When access to any confidential information is required, employees must request it from the management team.
- SWAAT will provide training to all employees to help them understand their responsibilities when handling data.
- In particular, strong passwords must be used and they should never be shared or written down.
- Personal data should not be disclosed to unauthorized persons, either within the company or externally.
- Data should be regularly reviewed and updated if it is found to be out of date. If it is no longer required, it should be deleted and disposed of in line with the Erasure Policy.
- Employees should request help from the management team or the data protection officer if they are unsure about any aspect of data protection.

#### 4.3.3 Data storage

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

When data is stored on paper, it should be kept in the secure cabinets, where unauthorized persons cannot gain access to 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 draw or filing cabinet.
- Employees should make sure paper and printouts are not left where unauthorized persons could see them, like on the printer or photocopier.

- Data printouts should be shredded and disposed of securely when no longer required.

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

- Data should be protected by strong passwords that are regularly changed and never shared or written down.
- When data is stored on removable media (like storage devices), these should be kept under lock and key when not in use.
- Data should only be stored on designated drives and servers, and should never be uploaded, unless onto the works server.
- Data clouds should not be used for storing any data.
- Our server is located in its own room, in a locked cabinet, away from the general office space and non-staff members.
- Data should be backed up nightly. These backups are checked and tested regularly.
- Data should never be saved directly onto laptops or other mobile device like tablets or smart phones.
- All servers and computers containing data are to be protected by approved security software and a firewall.

## **5 Data use**

Personal data is of no value to SWAAT unless the business needs it to ensure the requirements of the certification bodies are met. However, it is when personal data is accessed and used that it is at 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.
- Data must be encrypted before being transferred electronically and only to authorised external contacts.
- Personal data should never be transferred outside the European Economic Area.
- Employees should not save copies of personal data to their own computers, tablets or phones. Always access and update the central copy of any data.

### **5.1 Data Accuracy**

The law requires that SWAAT is to take reasonable steps to ensure data is kept accurate and up-to-date.

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

It is the responsibility of all employees who work with the data to take reasonable steps to ensure that 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 on the database when they call.
- SWAAT will make it easy for data subjects to update the information SWAAT holds about them.
- Data should be updated as inaccuracies are discovered. For instance, if a customer can no longer be reached on their stored telephone number or address, it should be removed from the database.
- It is the admin's responsibility to check and ensure that the databases are checked against the suppression files every six months.

## 5.2 Subject Access Requests

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

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

If any 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 Admin Staff, at [info@swaat.co.uk](mailto:info@swaat.co.uk). The admin team will then bring the request to the attention of the management team, who will invite the individual into SWAAT, where they can review the information kept about them on the database. This is a protection measure to ensure that information is requested by the individual alone and not inadvertently shared with others. We keep photographic evidence of all individuals and this will form the check against their personal data file.

Individuals will be charged £25 per subject access request, the individual will be invited into SWAAT within 14-working-days of the request (subject to bank holidays and holy days). Individuals will need to bring photographic evidence.

The identity of the individuals will be checked against the information held on file, so for example, photos, driving licence, passports, etc.

## 6 Disclosing data for other reasons

In certain circumstances, the Data Protection Act allows personal data to be disclosed to law enforcement agencies without the consent of the data subject.

Under these circumstances SWAAT will disclose requested data. However, the management team will ensure that the request is legitimate, seeking assistance from the company's legal advisors where necessary.

## 6.1 Providing information

SWAAT aims to ensure that individuals are aware that their data is being processed and that they understand:

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

## 6.2 Privacy Statement under GDPR

Articles 12, 13 and 14 of the GDPR outline the requirements on giving privacy information to data subjects.

These are more detailed and specific than in the UK Data Protection Act 1998 (DPA).

The GDPR says that the information you provide must be:

- Concise, transparent, intelligible and easily accessible;
- Written in clear and plain language, particularly if addressed to a child; and
- Free of charge

# 7 Privacy Statement

## 7.1 Privacy Notice

1. As an employer, SWAAT needs to keep and process information about employees for normal employment purposes. The information we hold and process will be used for our management and administrative use only. We will keep and use it to enable us to run the business and manage our relationship with you effectively, lawfully and appropriately, during the recruitment process, whilst you are working for us, at the time when your employment ends and after you have left. This includes using information to enable us to comply with the employment contract, to comply with any legal requirements, pursue the legitimate interests of the Company and protect our legal position in the event of legal proceedings. If you do not provide this data, we may be unable in some circumstances to comply with our obligations and we will tell you about the implications of that decision.
2. As a company pursuing training and assessment activities, we need to process candidate data to pursue our legitimate business interests, for example to prevent fraud, administrative purposes or ensure certification. The nature of our legitimate interests are certification and ensuring identification. We will never process your data where these interests are overridden by your own interests.
3. All of the information we hold will have been provided by you.
4. The information we hold includes your:
  - Booking form
  - Application form
  - Results form
  - Contract to provide training/assessment/services requested
  - All certification paperwork provided

All this information is held on a password protected database, it is used to ensure we meet our legal responsibilities, but, also to update you when your qualifications or training becomes out of date and to inform you of changes to industry changes and updates via a newsletter sent out up to six times a

year. If you do not want the updates newsletter please email us and let us know and we will take that preference off of the database: [info@swaat.co.uk](mailto:info@swaat.co.uk) .

5. We do not personal process any special categories of information relating to your racial or ethnic origin, however, the certification bodies that we deal with may capture and use that information. For more information on this please email and we will send you a list of the organisations who collect this information for their own records: [info@swaat.co.uk](mailto:info@swaat.co.uk) .
6. Other than as mentioned below, we will only disclose information about you to third parties if we are legally obliged to do so or where we need to comply with our contractual duties to you, for instance we may need to pass on certain information to your employer.
7. We transfer all assessment paperwork to the relevant certification bodies, with whom your qualification is certificated. For more information on this please email and we will send you their contact information: [info@swaat.co.uk](mailto:info@swaat.co.uk) .
8. We will never pass your information on to any third party group/individual, or sell your information, your information which we hold will never be sent out of the building, unless required by law or requested by the certification body you have requested certification from.
9. We do use automated decision making (including profiling).
10. Your personal data will be stored for as long as the business is functioning or until you or your representative requests that you are removed, please let us know by emailing [info@swaat.co.uk](mailto:info@swaat.co.uk) . All paper records are stored electronically and the paper versions deleted after a two year period, data after this stage is stored electronically for a period of six years, after this time it is deleted in accordance with our erasure policy.
11. If in the future we intend to process your personal data for a purpose other than that which it was collected we will provide you with information on that purpose and any other relevant information.
12. Under the General Data Protection Regulation (GDPR) and The Data Protection Act 2018 (DPA) you have a number of rights with regard to your personal data. You have the right to request from us access to and rectification or erasure of your personal data, the right to restrict processing, object to processing as well as in certain circumstances the right to data portability.
13. If you have provided consent for the processing of your data you have the right (in certain circumstances) to withdraw that consent at any time which will not affect the lawfulness of the processing before your consent was withdrawn.
14. You have the right to lodge a complaint to the Information Commissioners' Office if you believe that we have not complied with the requirements of the GDPR or DPA 18 with regard to your personal data.
15. SWAAT is the controller and processor of data for the purposes of the DPA 18 and GDPR.
16. If you have any concerns as to how your data is processed you can contact us on [info@swaat.co.uk](mailto:info@swaat.co.uk) or write to us at SWAAT, 1 Owen Sivell Close, Liskeard Business Park, Liskeard, PL14 3US.