Document	Title:	Revision
UK.P.015-POL-25	Privacy and Personal Data Protection Policy	6.0
P015 - Information Security BMS		

Process owner: IT Manager \ HR Manager		Signature: (*electronic permissible*)
Prepared by: Simon Arnold	**Date prepared:** 27-Dec-2025	
Approved by: Lisa Alexander	**Date approved:** 26-Jan-2026	

Revision History

Revision	Date	Description of changes	Requested by
A	18 Jul 19	Original	Jon Smith
B	10 Dec 19	Updated cross references	Jon Smith
3.0	Sep 21	Uploaded to SharePoint DMS	Jon Smith
4.0	28 Jun 22	Updated cross references	Jon Smith
5.0	25-Feb-2025	"UK-"Prefix added (as per BMS procedure to globally update all prefixes "HK or UK") Contents table changed	Robin Huddleston / Simon Arnold
6.0	23-Dec-2025	Review, grammar	Simon Arnold

1.0 Purpose

The purpose of this policy is to set out the relevant legislation and to describe the steps Surface Technology International Limited is taking to ensure that it complies with it.

2.0 Scope

This control applies to all systems, people and processes that constitute the organisation's information systems, including board members, directors, employees, suppliers and other third parties who have access to Surface Technology International Limited systems in relation to European and United Kingdom personnel.

Contents

3.0 Policy

Privacy and protection of personally identifiable information shall be ensured as required in relevant legislation and regulation where applicable

3.1 Introduction

In its everyday business operations STI makes use of a variety of data about identifiable individuals, including data about:

- Current, past and prospective employees
- Customers
- Users of its websites
- Other stakeholders

In collecting and using this data, the organisation is subject to a variety of legislation controlling how such activities may be carried out and the safeguards that must be put in place to protect it. The purpose of this policy is to set out the relevant legislation and to describe the steps STI is taking to ensure that it complies with it.

3.2 Privacy and Personal Data Protection Policy

The General Data Protection Regulation\Data Protection Act 2018

The General Data Protection Regulation 2018 (GDPR) otherwise known as the Data Protection Act 2018, is one of the most significant pieces of legislation affecting the way that Surface Technology International Limited carries out its information processing activities. Significant fines are applicable if a breach is deemed to have occurred under the GDPR, which is designed to protect the personal data of citizens of the European Union. It is Surface Technology International Limited's policy to ensure that our compliance with the GDPR and other relevant legislation is clear and demonstrable at all times.

3.3 Definitions

There is a total of 26 definitions listed within the GDPR and it is not appropriate to reproduce them all here. However, the most fundamental definitions with respect to this policy are as follows:

Personal data is defined as:*'any information relating to an identified or identifiable living person ('data subject'); an identifiable living person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person;'*

'processing' means:

'any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;'

'controller' means:

'the living or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law;'

3.4 Principles Relating to Processing of Personal Data

There are several fundamental principles upon which the GDPR is based. These are as follows:

Personal data shall be:

a. processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency');

b. collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be incompatible with the initial purposes ('purpose limitation');

c. adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');

d. accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy');

e. 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; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('storage limitation');

f. 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 ('integrity and confidentiality').

The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability').

STI must ensure that it complies with all of these principles both in the processing it currently carries out and as part of the introduction of new methods of processing such as new IT systems. The operation of an information security management system (ISMS) that conforms to the ISO/IEC 27001 international standard is a key part of that commitment.

3.5 Rights of the Individual

The data subject also has rights under the GDPR. These consist of:

1. The right to be informed
2. The right of access
3. The right to rectification
4. The right to erasure
5. The right to restrict processing
6. The right to data portability
7. The right to object
8. Rights in relation to automated decision making and profiling.

Each of these rights must be supported by appropriate procedures within STI that allow the required action to be taken within the timescales stated in the GDPR.

These timescales are shown in Table 1.

Data Subject Request	Timescale
The right to be informed	When data is collected (if supplied by data subject) or within one month (if not supplied by data subject)
The right of access	One month
The right to rectification	One month
The right to erasure	Without undue delay
The right to restrict processing	Without undue delay
The right to data portability	One month
The right to object	On receipt of objection

Rights in relation to automated decision making and profiling.	Not specified

3.6 Consent

Unless it is necessary for a reason allowable in the GDPR, explicit consent must be obtained from a data subject to collect and process their data. Transparent information about our usage of their personal data must be provided to data subjects at the time that consent is obtained and their rights with regard to their data explained, such as the right to withdraw consent. This information must be provided in an accessible form, written in clear language and free of charge. If the personal data is not obtained directly from the data subject, then this information must be provided within a reasonable period after the data are obtained and definitely within one month.

3.7 Privacy by Design

STI has adopted the principle of privacy by design and will ensure that the definition and planning of all new or significantly changed systems that collect or process personal data will be subject to due consideration of privacy issues, including the completion of one or more privacy impact assessments.

The privacy impact assessment will include:

- Consideration of how personal data will be processed and for what purposes
- Assessment of whether the proposed processing of personal data is both necessary and proportionate to the purpose(s)
- Assessment of the risks to individuals in processing the personal data
- What controls are necessary to address the identified risks and demonstrate compliance with legislation

Use of techniques such as data minimisation and pseudonymisation should be considered where applicable and appropriate.

3.8 Transfer of Personal Data

Transfers of personal data outside the European Union must be carefully reviewed prior to the transfer taking place to ensure that they fall within the limits imposed by the GDPR. This depends partly on the European Commission's judgement as to the adequacy of the safeguards for personal data applicable in the receiving country and this may change over time.

Intra-group international data transfers must be subject to legally binding agreements referred to as Binding Corporate Rules (BCR) which provide enforceable rights for data subjects.

3.9 Data Protection Officer

A defined role of Data Protection Officer (DPO) is required under the GDPR if an organisation is a public authority, if it performs large scale monitoring or if it processes particularly sensitive types of data on a large scale. The DPO is required to have an appropriate level of knowledge and can either be an in-house resource or outsourced to an appropriate service provider.

Based on these criteria, Surface Technology International Limited does not require a Data Protection Officer to be appointed however this is a dual role undertaken between HR Manager and IT Manager.

3.10 Breach Notification

It is STI's policy to be fair and proportionate when considering the actions to be taken to inform affected parties regarding breaches of personal data. In line with the GDPR, where a breach is known to have occurred which is likely to result in a risk to the rights and freedoms of individuals, the relevant Data Protection Authority (DPA) will be informed within 72 hours. This will be managed in accordance with our Information Security Incident Response Procedure which sets out the overall process of handling information security incidents. Under the GDPR the relevant DPA has the authority to impose a range of fines of up to four percent of annual worldwide turnover or twenty million Euros, whichever is the higher, for infringements of the regulations.

3.11 Addressing Compliance to the GDPR

The following actions are undertaken to ensure that Surface Technology International Limited always complies with the accountability principle of the GDPR:

- The legal basis for processing personal data is clear and unambiguous
- All staff involved in handling personal data understand their responsibilities for following good data protection practice
- Training in data protection has been provided to all staff via the annual refresher security training
- Rules regarding consent are followed
- Routes are available to data subjects wishing to exercise their rights regarding personal data and such enquiries are handled effectively
- Regular reviews of procedures involving personal data are carried out
- Privacy by design is adopted for all new or changed systems and processes
- The following documentation of processing activities is recorded:
    - Organisation name and relevant details
    - Purposes of the personal data processing
    - Categories of individuals and personal data processed
    - Categories of personal data recipients
    - Agreements and mechanisms for transfers of personal data to non-EU countries including details of controls in place
    - Personal data retention schedules
    - Relevant technical and organisational controls in place

These actions will be reviewed on a regular basis as part of the management review process of the information security management system.

4.0 Roles and Responsibilities

4.1 Employee

All employees and contractors / suppliers / customers / agency workers have a responsibility to ensure that they adhere to this policy.

4.2 Line Managers

It is the Line Manager's responsibility to ensure the policy is adhered to for any employee within their department and contractors / suppliers / customers / agency workers working within their department.

4.3 Senior Management Team / Directors

It is the Senior Management Team / Director's responsibility to ensure the policy is fairly and consistently adhered to and that there is a culture that supports the application of this policy.

4.4 Human Resources

It is Human Resources responsibility to ensure the fair and consistent application of this policy, providing guidance where necessary.

5.0 Breach of Policy

A breach of this policy by any employee may result in appropriate disciplinary action being taken.

6.0 Related Policies

- ISO27001:2022 - A.5.34 Privacy and protection of personally identifiable information (PII).
- UK-P.015-PRO-17 Information Classification Procedure
- UK-P.015-PRO-08 Information Labelling Procedure
- UK-F.015-11 Personal Commitment Statement
- UK-P.015-POL-05 Electronic Messaging Policy
- UK-P.015-POL-36 Internet Acceptable Use Policy
- UK-P.015-PRO-02 Information Security Incident Response Procedure
- UK-P.015-POL-07 Information Security Roles, Responsibilities and Authorities
- UK-F.015-46 PII Register and Internal Privacy Notice Summary
- UK-P.015-POL-24 Records Retention and Protection Policy

7.0 Review Frequency

This policy will be reviewed every 3 years