



1 SCOPE AND PURPOSE

This policy sets out to outline how Total Solutions Technology (TST) process personal data in manual and electronic records. It also covers our response to any data breach and other rights under the General Data Protection Regulation (GDPR) and current Data Protection Act.

This policy applies to the personal data of job applicants, existing and former employees, volunteers, placement students and self-employed contractors. These are referred to in this policy as relevant individuals.

TST recognises it has a duty of trust and confidence to its employees, customers and business partners in its supply chain. TST pledge to remain updated with current laws and legislation regarding GDPR, to exercise the requirements needed to be a compliant employer and will challenge individuals and related situations where applicable.

Contents

1	Scope and Purpose	1
2	Useful Contacts	2
3	Types of Data Held by TST	2
4	Definitions.....	2
5	Data Protection Principles	3
6	Data Disclosures.....	3
7	Responsibility.....	4
8	Records	5
9	Breach Procedures.....	5
10	Whistleblowing.....	5



2 USEFUL CONTACTS

Managing Director for TST

Paul Jones, Managing Director

Email: paul.jones@tst.co.uk

Telephone: 01462 557455

Address: Total Solutions Technology

5-6 Amor Way, Letchworth Garden City

Hertfordshire SG6 1UG

Data Protection Officer for TST

Tyler Simon, Head of People and Quality

Email: tyler.simon@tst.co.uk

Telephone: 01462 557455

Address: Total Solutions Technology

5-6 Amor Way, Letchworth Garden City

Hertfordshire SG6 1UG

3 TYPES OF DATA HELD BY TST

Further information on the types of data TST hold can be found within their respective notices, policies and statements in the GDPR category. Relevant individuals should refer to our privacy notice for more information.

4 DEFINITIONS

'Personal data' is information that relates to an identifiable person who can be directly or indirectly identified from that information. Examples include a person's name, identification number, location or online identifier. It can also include pseudonymised data.

'Special categories of personal data' is data which relates to an individual's health, sex life, sexual orientation, race, ethnic origin, political opinion, religion, and trade union membership. It also includes genetic and biometric data (where used for ID purposes.)

'Criminal offence data' is data which relates to an individual's criminal convictions and offences.

'Data processing' is 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.



5 DATA PROTECTION PRINCIPLES

All personal data obtained will:

- Be processed fairly, lawfully and in a transparent manner.
- Be collected for specific, explicit, and legitimate purposes.
- Be adequate, relevant and limited to what is necessary for the purposes of processing.
- Be kept accurate and up to date and every reasonable effort will be made to ensure that inaccurate data is rectified or erased without delay.
- Not be kept for longer than is necessary for its given purpose.
- Be processed in a manner that ensures appropriate security of personal data including protection against unauthorised or unlawful processing, accidental loss, destruction or damage by using appropriate technical or organisation measures.
- Comply with the relevant data protection procedures for international transferring of personal data.

In addition, personal data will be processed in recognition of an individuals' data protection rights, as follows:

- The right to be informed.
- The right of access.
- The right for any inaccuracies to be corrected.
- The right to have information deleted.
- The right to restrict the processing of the data.
- The right to portability.
- The right to object to the inclusion of any information.
- The right to regulate any automated decision-making and profiling of personal data.

6 DATA DISCLOSURES

TST may be required to disclose certain data to any person. A disclosure will only be made when it is strictly necessary for its purpose. The circumstances leading to such disclosures include:

- Any employee benefits operated by third parties.
- Disabled individuals, where any reasonable adjustments are required to assist them at work.
- Individuals' health data, to comply with health and safety or occupational health obligations towards the employee.
- For Statutory Sick Pay purposes.
- To TST's HR Management and Administration Teams, to consider how an individual's health affects their ability to do their job.
- The smooth operation of any employee insurance policies or pension plans.



7 RESPONSIBILITY

TST have onboarded a Data Protection Officer (DPO) to protect the personal data of relevant individuals, which TST hold or to which we have access. The DPO has specific responsibilities for:

- The processing and controlling of data.
- The comprehensive reviewing and auditing of its data protection systems and procedures.
- Reviewing the effectiveness and integrity of all the data that must be protected.

The DPO provides information to its employees on their data protection rights, how it uses their personal data, and how it protects it. The information includes the actions relevant individuals can take if they think that their data has been compromised in any way. They will provide its employees with information and training to make them aware of the importance of protecting personal data, to teach them how to do this, and to understand how to treat information confidentially. The DPO can account for all personal data it holds, where it comes from, who it is shared with and also who it might be shared with.

The DPO will carry out risk assessments as part of its reviewing activities to identify any vulnerabilities in its personal data handling and processing, and to take measures to reduce the risks of mishandling and potential breaches of data security. The procedure includes an assessment of the impact of both use and potential misuse of personal data in and by TST. They recognise the importance of seeking individuals' consent for obtaining, recording, using, sharing, storing and retaining their personal data, and regularly reviews its procedures for doing so, including the audit trails that are needed and are followed for all consent decisions. We understand that consent must be freely given, specific, informed and unambiguous. We will seek consent on a specific and individual basis where appropriate. Full information will be given regarding the activities about which consent is sought. Relevant individuals have the absolute and unimpeded right to withdraw that consent at any time.

In addition, all employees of TST have a responsibility for data security and we mandate they commit to the following:

- Ensure that all files or written information of a confidential nature are stored in a secure manner and are only accessed by people who have a need and a right to access them.
- Ensure that all files or written information of a confidential nature are not left where they can be accessed by unauthorised people.
- Refrain from sending emails containing sensitive work-related information to their personal email address.
- Check regularly on the accuracy of data being entered on to.
- Always use the passwords provided to access the computer system and not abuse them by passing them on to people who should not have them.
- Ensuring that data is recorded on such devices only where absolutely necessary.
- Using an encrypted system.
- Ensuring that laptops or USB drives are not left lying around where they can be stolen.



8 RECORDS

We keep a record of our processing activities as per listed below. These records will be kept up to date so that they reflect current processing activities.

- Description of personal data shared.
- Owner(s) of the data.
- Purpose of processing data.
- Legal basis for processing data.
- Category type of recipient receiving data.
- Information regarding data being transmitted internationally.
- Retention period of the data.

9 BREACH PROCEDURES

TST have appropriate mechanisms for detecting, reporting and investigating suspected or actual personal data breaches, including security breaches. TST is aware of its duty to report significant breaches that cause significant harm to the affected individuals to the Information Commissioner's Office (ICO) and is aware of the possible consequences.

Where a data breach is likely to result in a risk to the rights and freedoms of individuals, it will be reported to ICO within 72 hours of us becoming aware of it and may be reported in more than one instalment. Individuals will be informed directly in the event that the breach is likely to result in a high risk to the rights and freedoms of that individual. If the breach is sufficient to warrant notification to the public, we will do so without undue delay.

10 WHISTLEBLOWING

If an issue requires whistleblowing to a regulatory body, these issues should be raised to the ICO.