



RTT SERVICES SOUTH LTD

RTT Services Data Protection and Information Security Policy

1. Introduction

RTT Services recognises that information and associated processes, systems, and networks are valuable assets. We are committed to ensuring the confidentiality, integrity, and availability of personal data in compliance with the Data Protection Act 1998 and the General Data Protection Regulations (GDPR) 2018. This policy sets out our approach to information security and data protection, ensuring that data is protected against unauthorised access, disclosure, and loss.

2. Purpose of the Policy

The purpose of this policy is to ensure that RTT Services complies with GDPR and other relevant data protection legislation. It defines the roles and responsibilities for handling personal and sensitive data, as well as the guidelines for ensuring the security and availability of our information systems.

3. Definition of Information Security

For the purposes of this policy, information security is defined as:

- **Preservation of Confidentiality:** Ensuring that personal and business data is only accessible by authorised individuals.
- **Protection Against Unauthorised Access and Disclosure:** Safeguarding data from being accessed or disclosed without permission.
- **Safeguarding Accuracy and Completeness:** Ensuring the accuracy and integrity of the information and its associated processing methods.
- **Ensuring Availability:** Ensuring that information and associated services are available to authorised users whenever needed.

4. Data Processing and Handling

RTT Services holds and processes information about employees, customers, and enquirers for legitimate commercial purposes. We are committed to ensuring that personal data is processed in compliance with GDPR, meaning:

- Data is collected lawfully, fairly, and transparently.
- Data is processed only for specified, legitimate purposes.
- The amount of data collected and processed is kept to the minimum necessary for the intended purpose.
- Data is kept accurate and up to date.
- Data is retained only for as long as necessary and is securely deleted or anonymised thereafter.

All staff are briefed on data protection requirements during induction, including:

- The **Employee Privacy Notice**, which is displayed on the company noticeboard.
- The **Customer Privacy Notice**, which is provided to enquirers and customers along with business terms and conditions, detailing how data is collected, stored, used, and handled.



5. Responsibilities

All employees, contractors, and third parties handling personal data or using RTT Services' information systems are expected to observe the information security policies and procedures during and after their time with the organisation. The supervision and enforcement of this policy are the responsibility of the Director.

6. IT Facility Usage

Company IT facilities must only be used for authorised purposes. Any unauthorised access or use of IT facilities is prohibited and may lead to disciplinary and legal proceedings. The Company reserves the right to monitor and investigate IT usage to ensure compliance with this policy.

Monitoring and Inspection:

- Operational logs may be inspected by authorised personnel such as computer operators and system administrators.
- Disclosure of information from logs will occur:
 - When required by law.
 - If a violation of law or company policy is suspected.
 - In cases where failure to act may result in bodily harm, property loss, or significant liability.

While user privacy is respected, the Company reserves the right to examine systems, directories, and files to ensure legal and policy compliance. Access to such data is limited and only permissible with authorisation from the Director or their nominee.

7. Software and Licensing Compliance

RTT Services ensures that all software and licensed products comply with the Copyright, Designs, and Patents Act 1988 and its subsequent amendments. Regular audits are carried out to ensure that only authorised software is in use within the organization. Unauthorised copying or use of software will be subject to disciplinary and legal proceedings.

8. IT Security Measures

To protect against malicious software and unauthorised external access to company networks and systems, RTT Services implements the following controls:

- **Firewalls:** Robust firewalls are in place to prevent unauthorised network access.
- **Antivirus and Anti-malware Protection:** All devices are equipped with up-to-date antivirus software and best practices for virus protection are enforced.
- **Password Protection:** All IT systems, laptops, and mobile devices must be password-protected to ensure only authorised users can access them.

9. Security Incident Reporting

All employees are responsible for reporting any suspected security incidents, vulnerabilities, or threats to the Directors immediately. This includes breaches of company security policies, system or service vulnerabilities, or observed security weaknesses.

Software malfunctions should also be reported to the Directors promptly to ensure timely resolution.



10. Disposal of Information

All employees have a responsibility to ensure that security is maintained when disposing of information. This includes securely deleting electronic data and properly disposing of physical documents in accordance with company procedures.

11. Breach Management

In the event of a data breach, RTT Services will follow its breach reporting and management procedure:

- **Reporting:** Staff must report any breach immediately to the Data Protection Officer (DPO).
- **Assessment:** The DPO will assess the breach and determine the appropriate course of action.
- **Notification:** If applicable, the breach will be reported to relevant authorities and affected individuals within 72 hours.

12. Data Protection Training

All staff receive mandatory data protection training during induction and regular refresher training thereafter. This training covers:

- The importance of data protection and security.
- The proper handling and storage of personal data.
- How to report incidents and breaches.

13. Policy Review

This Data Protection and Information Security Policy is subject to regular review to ensure compliance with relevant laws and regulations. Any updates will be communicated to all staff and stakeholders.

Signed:

Jake Davies

Director

RTT Services South Ltd

27/01/2026