QUALITY & SERVICE LIMITED *DATA PROTECTION POLICY STATEMENT*

INTRODUCTION

Quality & Service Limited needs to gather and use certain information about individuals. These can include clients, suppliers, business contacts, employees and other people the organisation has a relationship with or may need to contact.

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

WHY THIS POLICY EXISTS

This data protection policy ensures Quality and Service Limited:

- Complies with data protection law and follows good practice
- Protects the rights of employees, clients and partners
- Is open about how it stores and processes individuals' data
- Protects itself from the risk of a data breach

DATA PROTECTION LAW

The Data Protection Act 1998 describes how organisations, including Q&S, must collect, handle and store personal information. These rules apply regardless of whether data is stored electronically, on paper or on other materials. To comply with the law, personal information must be collected and uses fairly, stored safely and not disclosed unlawfully.

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

- Be processed fairly and lawfully
- Be obtained only for specific, lawful purposes
- Be adequate, relevant and not excessive
- Be accurate and kept up to date
- Not be held for any longer than necessary
- Processed in accordance with the rights of the data subjects
- Be protected in appropriate ways
- Not be transferred outside the European Economic Area (EEA), unless that country or territory also ensures an adequate level of protection

POLICY SCOPE

This policy applies to:

- The head office of Quality & Service Limited
- All offices of Quality & Service Limited
- All employees and volunteers of Quality & Service Limited
- All contractors, suppliers and other persons working on behalf of Quality & Service Limited

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 can include:

- Names of individuals
- Postal addresses
- Email addresses
- Telephone numbers
- Plus, any other information relating to individuals

DATA PROTECTION RISKS

This policy helps protect Quality & Service from some 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 the company uses data relating to them.
- **Reputational damage.** For instance, the company could suffer if hackers successfully gained access to sensitive data.

RESPONSIBILITIES

Everyone who works for or with Quality & Service has some responsibility for ensuring data is collected, stored and handled appropriately. Each office that 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 directors are ultimately responsible for ensuring that Quality & Service meets its legal obligations.

- The data protection officer, Nicola Rasul, is responsible for:
  - Keeping the directors updated about data protection responsibilities, risks and issues
  - Reviewing all data protection procedures and related policies, in line with an agreed schedule.
  - Handling data protection questions from employees and anyone else covered by this policy.
  - Dealing with requests from individuals to see the data Quality & Service holds on them (also called 'subject access requests')
  - Checking and approving any contracts or agreements with third parties that may handle company's sensitive data.
  - Perform regular checks and scans to ensure security hardware and software is functioning properly
  - Approving any data protection statements attached to communications such as email and letters.
  - Where necessary, working with other employees to ensure marketing initiatives abide by data protection principles.

GENERAL EMPLOYEE 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 confidential information is required, employees can request it from their line managers.
- **Quality & Service will provide training** to all employees to help them understand their responsibilities when handling data.
- Employees should keep all data secure, by taking sensible precautions and following the guidelines below.
- In particular, **strong passwords must be used** and they should not be shared.
- Personal data **should not be disclosed** to unauthorized people, either within the company or externally.
- Data should be **regularly reviewed and updated** if it is found to be out of date. If no longer required it should be deleted and disposed of.

DATA STORAGE

These rules describe how and where data should be safely stored. Questions about storing data safely can be directed to a managing director or the data protection officer.

When data is **stored on paper**, it should be kept in a secure place where unauthorised people cannot see or easily access it.

The 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 drawer or filing cabinet
- Employees should make sure paper and printouts and **not left where unauthorised people could see them**, like on a printer.
- **Data printouts should be shredded** and disposed of securely when no longer required.

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

- Data should be **protected by strong passwords** that are changed regularly and never shared between employees.
- If data is **stored on removable media** (Cd, DVD, USB), these should be kept locked away securely when not in use.
- Data should only be stored on **designated drives and servers**, and should only be uploaded to an **approved cloud computing services.**
- Servers containing personal data should be **sited in a secure location**, away from general office space.
- Data should be **backed up frequently**. Those backups should be tested regularly, in line with the company's standard backup procedures.
- Data should **never be saved directly** to laptops or other mobile devices like tablets or smart phones.
- All servers and computers containing data should be protected by **approved security software and a firewall.**

DATA USE

Personal data is of no value to Quality & Service unless the business can make us of it. However, it is when personal data is accesses and used that it can be at the 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.**
- Personal data should **never be transferred outside of the European Economic Area.**
- Employees **should not save copies of personal data to their own computers**. Always access and update the central copy of any data.

DATA ACCURACY

The law requires Quality & Service 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 Quality & Service should put into ensuring its accuracy.

It is the responsibility of all employees who work with data to take reasonable steps to ensure it is kept as accurate and up to date as possible.

- Data will be held in **as few places as necessary.** Employees should not create any unnecessary additional data sets.
- Employees should **take every opportunity to ensure data is updated.** For instance, by confirming a client's details when they call.
- Quality & Service will make it **easy for data subjects to update the information** it holds for them.
- Data should be **updated as inaccuracies are discovered**. For instance, if a client can no longer be reached on the stored telephone number, it should be removed from the database.

DISCLOSING DATA

All individuals who are the subject of personal data held by Quality & Service are entitled to:

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

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, Quality & Service will disclose requested data. However, it will ensure the request is legitimate, seeking assistance from the directors and the company's legal advisors where necessary.

Quality and Service 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

To these ends, the company has a privacy statement, setting out how data relating to individuals is used by the company.

We will review this policy as necessary. Copies are available upon request.

Managing Director ***Date: 02/01/2025***