



RSC Body Centre Limited
Smithfield Rd,
Market Drayton
TF9 1EW

Tel: 01630 655311
email: info@rscbodycentre.co.uk

RSC Body Centre Limited.
Company Registered in England and Wales, Number: 08393029
Trading as RSC Body Centre

Privacy Policy – November 2018

Introduction

RSC Body Centre Limited needs to gather and use certain information about individuals.

These can include customers, 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 business's data protection standards and comply with the law.

Why do we have a data protection policy?

This data protection policy ensures RSC Body Centre Limited:

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

Data Protection Law

The Data Protection Act 1998 and the General Data Protection Regulation (GDPR) describe how organisations 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 used fairly, stored safely and not disclosed unlawfully.

The Data Protection Act 1998 and General Data Protection Regulation (GDPR) are underpinned by eight important principles. These say 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 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

Risks and responsibilities

This Policy applies to:

- All employees and the director of RSC Body Centre Limited.
- All third party companies, suppliers and other people working on our behalf.

It applies to all data that the firm holds relating to the identifiable individuals. This can include:

- Names of individuals
- Postal addresses
- Email addresses
- Telephone numbers
- Vehicle registration
- Plus, any other information required for a quotation or claim.

Data protection risks

This policy helps to protect RSC Body Centre Limited 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 the firm uses data relating to them.
- Reputational damage. For instance, the company could suffer if hackers successfully gained access to sensitive data.

Our responsibilities

Everyone who works for RSC Body Centre Limited has some responsibility for ensuring data is collected, stored and handled appropriately.

Staff that handle personal data must ensure that it is handled and processed in line with this policy and data protection principles.

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.
- RSC Body centre Limited will provide training to 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 never be shared.
- Personal data should not be disclosed to unauthorised people, either within the firm 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.

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

These guidelines also apply to data that is usually stored electronically but has been printed out:

- When not required, the paper or file should be kept in a locked drawer or filing cabinet.
- Employees should make sure paper and printouts are 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.
- Data should only be stored on designated drives and servers.
- 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.
- All servers and computers containing data should be protected by approved security software and a firewall.

Data use

When personal data is accessed and used, 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.
- Employees should not save copies of personal data to their own computers. Always access and update the central copy of any data.
- Financial data must be encrypted before being transferred electronically.

Data Accuracy

The law requires RSC Body Centre Limited 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 RSC Body Centre Limited 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.
- Staff should take every opportunity to ensure data is updated. For instance, by confirming a customer's details when they call.
- Data should be updated as inaccuracies are discovered. For instance, if a customer can no longer be reached on their stored telephone number, it should be removed from the database.

Access Requests

All individuals who are the subject of personal data held by RSC Limited are entitled to:

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

The data controller will always verify the identity of anyone making a request for data before handing over any information.