Data Protection Policy

Context and overview

Key details

- Policy prepared by: Elizabeth Jackson
- Approved by board / management on: 01.05.18
- Policy became operational on: 01.05.18
- Next review date: 01.05.19

Introduction

Carpentry Joinery Services Limited needs to gather and use certain information about individuals.

These can include customers, suppliers, business contacts, employees and other people in the organisation they have 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 Carpentry Joinery Services Limited:

- Complies with data protection law and follow good practice
- Protects the rights of staff, customers and partners
- Is open about how it stores and processes individual's 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) describes how organisations – including Carpentry Joinery Services Limited – must collect, handle & store personal information.

These rules apply regardless of whether data is stored electronically, on paper, or other materials.

To comply with the law, personal information must be collected and used fairly, stored safely and no disclosed unlawfully.

The DPA / GDPR is underpinned by eight important principles. These say that personal data must:

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

People, risks and responsibilities

Policy scope

This policy applies to:

- The head office of Carpentry Joinery Services Limited
- All branches of Carpentry Joinery Services Limited
- All staff and volunteers of Carpentry Joinery Services Limited
- All contractors, suppliers and other people working on behalf of Carpentry Joinery Services 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 and GDPR 2018. 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 to protect Carpentry Joinery Services 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 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 Carpentry Joinery Services Limited has some responsibility for ensuring data is collected, stored and handled appropriately.

Each team that handles personal data must ensure that it is handled and processed in line with this policy and data protection principles.

- The **Company Director, Nigel Porter** is ultimately responsible for ensuring that Carpentry Joinery Services Limited meets its legal obligations.

- The **Office Manager, Elizabeth Jackson,** is responsible for:

    - Keeping the Managing Director updated about data protection responsibilities, risks and issues.
    - Reviewing all data protection procedures and related policies, in line with the agreed schedule.
    - Arranging data protection training and advice for the people covered by this policy.
    - Handling data protection questions from staff and anyone else covered by this policy
    - Dealing with requests from individuals to see the data Carpentry Joinery Services Limited holds about them (also called "subject access requests").
    - Checking or approving any contracts or agreements with third parties that may handle the company's sensitive data.

- The **IT/Marketing Manager, Lee Smith**, is responsible for:

    - Ensuring all systems, services and equipment used for storing data meet acceptable security standards.
    - Performing regular checks and scans to ensure security hardware and software is functioning properly.
    - Evaluating any third-party services the company is considering using to store or process data. For instance, cloud computing services.
    - Approving any data protection statements attached to communications such as e-mails and letters.
    - Addressing any data protection queries from journalists or media outlets like newspapers.
    - Where necessary, working with other staff to ensure marketing initiatives abide by 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**. When access to confidential information is required, employees can request it from their line managers.

- Carpentry Joinery Services Limited **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 should never be shared.

- Personal data **should not be disclosed** to unauthorised people, either within the company or externally.

- Date should be **regularly reviewed and updated** if it is found to be out of date. If no longer needed, it should be deleted and disposed of.

- Employees **should request help** from their line manager or the office manager if they are unsure about any aspect of data protection.

Data storage

These rules describe how and where data should be safely stored. Questions about storing data safely can be directed to the IT manager or Office Manager.

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 for some reason.

- When not required, the paper of files 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 authorised 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** (like a CD or DVD), these should be kept locked away securely when not being used.

- Data should only be stored on **designated drives and servers** and should only be uploaded to **an approved cloud computing service.**

- 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 smartphones.

- 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 Carpentry Joinery Services Limited unless the business can make use of it. However, it is when personal data is accessed 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.** The IT manager can explain how to send data to authorised external contacts.
- 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 Carpentry Joinery Services 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 Carpentry Joinery Services Limited should put into ensuring its accuracy.

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

- Data will be held in **as few places as necessary**. Staff should not create any unnecessary additional data sets.
- Staff should **take every opportunity to ensure data is updated.** For instance, by confirming a customer's details when they call.
- Carpentry Joinery Services Limited will make it **easy for data subjects to update the information** Carpentry Joinery Services Limited holds about them.
- 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.
- It is the marketing manager's responsibility to ensure **marketing databases are checked against industry suppression files** every six months.

Subject access requests

All individuals who are the subject of personal data held by Carpentry Joinery Services Limited are entitled to:

- Ask **what information** the company 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 obligations.**

If an individual contacts the company requesting this information, this is called a subject access request.

Subject access requests from individuals should be made by e-mail, addressed to the Office Manager at liz@cjshalifax.co.uk. The data controller can supply a standard request form, although individuals to not have to use this.

Individuals will be charged £10 per subject access request. The Office Manager will aim to provide the relevant data within 14 days.

The Office Manager will always verify the identity of anyone making a subject access request before handing over any information.

Disclosing data for other reasons

In certain circumstances, the Data Protection Act/GDPR allows personal data to be disclosed to law enforcement agencies without the consent of the data subject.

Under these circumstances, Carpentry Joinery Services Limited will disclose requested data. However, the Office Manager will ensure the request is legitimate, seeking assistance from the board and from the company's legal advisors where necessary.

Providing information

Carpentry Joinery Services Limited 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

[This is available upon request. A version of this statement is also available on the company's website]

Data disposal request

Carpentry Joinery Services Limited has a responsibility to dispose of your data safely and securely once it is no longer required.

You may make a request to have your data removed from our systems by means of a Subject Access Request (see above). Please note that whilst we will not “actively” use your data following completion of a project, we do have to “hold” basic information on file in line with GOV.UK guidelines:

- Financial records must be retained for a period of 6 years from the end of the financial year
- Payroll information must be kept for 3 years after dismissal

Once you make a request to remove your data from our database, we will inform you upon completion.