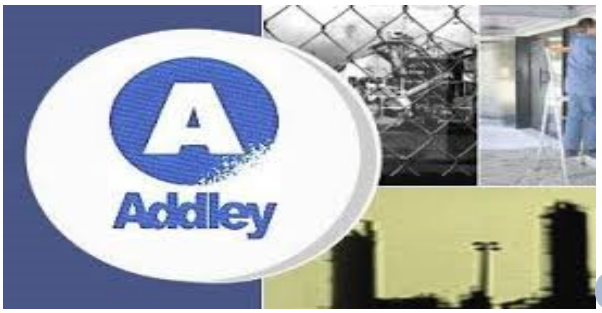

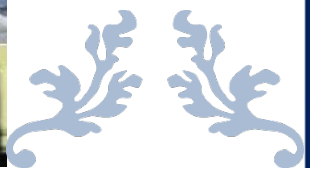

JDI Computer Services

DATA PROTECTION & INFORMATION SECURITY POLICY DOCUMENT

Data Protection Policy Document

This policy forms the companies Data Protection & Information Security Policy documentation.

JUNE 24, 2019

JDI COMPUTER SERVICES LIMITED
Registered Office: 5 Church Walk, Fulwood Row, Preston, Lancashire. PR2 6SZ

1.0 Introduction

John Addley 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 company's data protection standards — and to comply with the law.

1.1 Why does this policy exist

This data protection policy ensures John Addley 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 individuals' data
- Protects itself from the risks of a data breach

1.2 Data Protection Law

The Data Protection Act 1998, General Data Protection Regulation 2018 and the Data Protection Act 2018 describe how organisations — including John Addley Limited 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 & General Data Protection Regulation are 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

2.0 People, Risks and Responsibilities

2.1 Policy Scope

This policy applies to:

- The head office of John Addley Limited
- All branches of John Addley Limited
- All staff, sub-contractors and volunteers of John Addley Limited
- All contractors, suppliers and other people working on behalf of John Addley 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 2018 or the General Data Protection Regulation (2018). This can include:

- Names of individuals
- Postal addresses
- Email addresses
- Telephone numbers
- …plus any other information relating to individuals

2.2 Data protection risks

This policy helps to protect John Addley 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.

2.3 Responsibilities

Everyone who works for or with John Addley 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.

However, these people have key areas of responsibility:

• The **board of directors** is ultimately responsible for ensuring that John Addley Limited meets its legal obligations.

• The **[data protection officer] – Rose Hall,** (Supported by JDI Computer Services) are responsible for:

- Keeping the board updated about data protection responsibilities, risks and issues.
- Reviewing all data protection procedures and related policies, in line with an 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 John Addley Limited holds about them (also called 'subject access requests').
- Checking and approving any contracts or agreements with third parties that may handle the company's sensitive data.

• The [**IT manager], Rose Hall,** (Supported by JDI Computer Services) are 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.

• The **[marketing manager], Rose Hall,** (Supported by JDI Computer Services) are responsible for:

- Approving any data protection statements attached to communications such emails 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.

2.3 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.

• John Addley Limited **will provide training** to all employees to help them understand their responsibilities when handling all business sensitive and personal 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. Employees are forbidden from using any username / password used within the company externally. This also includes external work-based applications.

• Personal data **should not be disclosed** to unauthorised 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.

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

2.4 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 data controller.

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 or 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 or their desk. When printing business sensitive or personal data then the printouts must be collected immediately & accounted for.

• **Data printouts should be shredded** and disposed of securely when no longer required. The company's standard model is shredding by means of using a "Cross Shredder" or the companies recognised "Confidential Waste" provider.

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** (like a USB drive, CD or DVD), these should be kept locked away securely when not being used. All USB devices that have any Business Sensitive or Personal data on them **should be encrypted using Windows Bitlocker** encryption.

• 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 smart phones unless authorized by a company director.

• All servers and computers containing data should be protected by **approved security software and a firewall**.

2.5 Data Use

Personal data is of no value to John Addley 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. For staff using laptop devices (Bluetooth enabled) then 'Dynamic Locking' should be enabled to help further secure the device.

• Personal data **should not be shared informally**. In particular, it should never be embedded in the plain text of an email, as this form of communication is not secure. All personal data should be placed in a **password protected file** and the attached password protected file sent by email to the recipient.

• 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**. Should a company asset (E.G Laptop) be taken outside of Europe then the DPO should be notified prior to this happening.

• Employees **should save copies of personal data to their own computers where no centralised location is available.** They should always access and update the central copy of any data where possible.

2.6 Data accuracy

Keeping personal data accurate is very important to the company, John Addley Limited staff are expected to amend all personal data where it's found not to be accurate.

It is the responsibility of all staff 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 not create any unnecessary additional data sets. Where data is replicated to another device (on a temporary basis) then the temporary location should have all copies removed as soon as possible.

• Staff should **take every opportunity to ensure data is updated.** For instance, by confirming a customer's details when they call. This should happen at least once per year.

• John Addley Limited will make it **easy for data subjects to update the information** John Addley Limited holds about them. For instance, via the company website, or by writing to the head office in Chester.

• Data should be **updated as inaccuracies are discovered**. For instance, if a customer can no longer be reached on their stored telephone number / email, it should be removed from the database. You should also take steps to communicate with the customer and obtain updated details. Where required you should ensure that the rest of the company are made aware of the changes.

• It is the marketing manager's responsibility to ensure **marketing databases are checked against industry suppression files** every six months.

2.7 Subject access requests

All individuals who are the subject of personal data held by John Addley 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 protection obligations**.

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

Subject access requests from individuals should be made by email, addressed to the data controller at addleyaccounts@addley.co.uk - The data controller can supply a standard request form, although individuals do not have to use this.

Individuals may be charge £25 per subject access request where the request is deemed to be repetitive and the same data is being created. The data controller will aim to provide the relevant data within 28 days.

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

All Subject Access requests (SAR) must be passed to Rose Hall who will deal with the request and ensure that the required information is shared with the Data Subject. Not all information we hold about the Data Subject requires to be sent to the Data Subject. For further information then you should speak with Rose Hall.

2.8 Disclosing data for other reasons

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, John Addley Limited will disclose requested data. However, the data controller will ensure the request is legitimate, seeking assistance from the board and from the company's legal advisers where necessary. For further information then you should speak with Rose Hall.

2.9 Providing information

John Addley 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 on request. A version of this statement is also available on the company's website.]