Data Protection Policy

Introduction

TLJ Group Ltd needs to gather, store and use personal information about individuals.

These can include customers, suppliers, business contacts, employees and other people the organization has a relationship with or may need to contact. This information is stored on secure servers provided by ANS, a reputable cloud hosting provider based in the United Kingdom.

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

The data protection policy ensures TLJ Group Ltd:

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

Data Protection Law

The Data Protection Act 2018 (DPA), The Privacy and Electronic Communications Regulations (PECR) and The General Data Protection Regulations (GDPR) describe how organisations, including TLJ Group Ltd. Must collect, handle, use 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 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.

Policy Scope

This policy applies to:

- The head office of TLJ Group Ltd
- All employees of TLJ Group Ltd
- Customers and suppliers of TLJ Group Ltd

It applies to all data that the company holds relating to identifiable individuals, even if that information technically falls outside The Data Protection Act (DPA), The Privacy and Electronic Communications Regulations (PECR) and The General Data Protection Regulations (GDPR). This can include:

- Names of individuals
- Postal addresses
- Email addresses
- Telephone numbers
- Any other information relating to individuals

Data Protection Risks

This policy helps to protect TLJ Group Ltd 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 the 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 TLJ Group Ltd has some responsibility for ensuring data is collected, stored and handled appropriately.

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

However, these people have key areas of responsibility:

- The Directors are ultimately responsible for ensuring TLJ Group Ltd meets its legal obligations.

- The Data Protection Manager, is 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.

  Dealing with requests from individuals to see the data TLJ Group Ltd. holds about them (also called ‘subject access request).

Checking and approving any contracts or agreements with third parties that may handle the company's sensitive data.

- The Marketing Manager, is responsible for:

  Approving any data protection statements attached to communications such as emails and letters.

  Where necessary, working with other employees to ensure marketing initiatives abide by data protection principles.

  Addressing any data protection queries.

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 the management team.

TLJ Group Ltd will provide training to all employees to help them understand their responsibilities when handling data.

Employees should heel all data secure, by taking sensible precautions and following guidelines below.

In particular, strong passwords must be used and they should never 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.

Employees should request help from the management team or the data protection officers if they are unsure about any aspect of data protection.

Data Storage

These rules describe how and where data should be safely stored. Question about storing data safely can be directed to the Data Protection Manager.

When data is stored on paper, it should be kept in a secure place where unauthorized 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 files should be kept in a locked drawer or filing cabinet.
- Employees should make sure paper and printouts are not left where unauthorised people cannot see them.

- Data printouts should be shredded and disposed of securely when no longer required.

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

- Data should be protected by strong passwords that are changed regularly and never shared between colleagues.
- If data is stored on removable devises (like a USB, 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 devises 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 TLJ Group Ltd 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 Data Protection Officer can explain how to send data to authorized external contacts.
- Personal data should never be transferred electronically. The Data Protection Officer can explain how to end data to authorized external contacts.
- Persona data should ever 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 TLJ Group Ltd. 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 TLJ Group Ltd 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 not create unnecessary additional data sets.

- Data should be updated as inaccuracies are discovered. For instance, if a customer can no longer be reached on their stored telephone number, this should be removed from the database.

All individuals who are subject of personal data held by TLJ Group Ltd. 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 contacts the company requesting this information, this is called a subject access request.

Subject access requests from individuals should be made by email, addressed to support@tljgroup.com they can supply a standard request form, although individuals do not have to use this.

They will aim to provide the relevant data within 7 days.

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

In certain circumstances, The Data Protection Act (DPA), The Privacy and Electronic Communications Regulations (PECR) and The General Data Protection Regulations (GDPR) allows personal data to be disclosed to law enforcement agencies without the consent of the data subject.

Under these circumstances, TLJ Group Limited, will disclose requested data. However, the Data Protection Manager will ensure the request is legitimate, seeking assistance from the Directors and from legal advisers where necessary.

TJ Group 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

This Policy has been approved & authorised by:

Name: Claire Martin

Position: HSQE and HR Director

Date: 21st September 2026 To be reviewed: September 2027

Signature: