

Site Visitor Privacy Policy

This notice explains how we collect and use your personal data when you visit this site. Please read it before entering.

1. Who Controls Your Data

Thomas Johnstone Ltd is committed to protecting your personal information and respecting your privacy.

Thomas Johnstone Ltd is the data controller for personal data collected at this site, and can be contacted at:

Thomas Johnstone Ltd Cartside Avenue Inchinnan Business Park Renfrewshire PA4 9RU

Our Data Protection Officer is David Hadow (Joint Managing Director). You can contact the DPO at DPO@tjl.com or at the address above.

2. What Personal Data We Collect

When you access this site, we may collect the following types of personal data:

- Identity details – your full name, company name, job title, and identification documents.
- Contact details – phone number, email address, and emergency contact.
- Access records – date and time of entry and exit, vehicle registration, and access control data.
- Biometric data – facial biometric data for site access control, fire roll call / emergency evacuation, and timesheet / attendance management.
- Visual data – photographs and CCTV footage for safety and security monitoring.

Where we process special category data (including biometric data), this is done under the additional conditions set out in Article 9 of the UK GDPR, as described below.

We do not use your data for marketing purposes.

3. Why We Collect It and Our Legal Basis

The law requires us to have a legal basis for collecting and using your personal data. We rely on one or more of the following legal bases:

- Performance of a contract with you: Where we need to perform the contract we are about to enter into or have entered into with you.
- Legitimate interests: We may use your personal data where it is necessary to conduct our business and pursue our legitimate interests. We make sure we consider and balance any potential impact on you and your rights (both positive and negative) before we process your personal data for our legitimate interests. We do not use your personal data for activities where our interests are overridden by the impact on you (unless we have your consent or are otherwise required or permitted to by law).

- Legal obligation: We may use your personal data where it is necessary for compliance with a legal obligation that we are subject to. We will identify the relevant legal obligation when we rely on this legal basis.

Purposes for which we will use your personal data

We have set out below, in a table format, a description of all the ways we plan to use the various categories of your personal data, and which of the legal bases we rely on to do so. We have also identified what our legitimate interests are where appropriate.

PURPOSE	DATA COLLECTED	LEGAL BASIS
Maintaining fire roll-call and emergency evacuation capability	Sign-in and access records	Legal obligation (health and safety requirements)
Ensuring the safety and security of all individuals on site; confirming identity and authorisation for site access	Identity details and access records	Legitimate interests (protecting our sites, personnel and assets)
Site access control and fire roll call / emergency evacuation via the CloudPass facial recognition system	Facial biometric data	Legitimate interests (site safety and security); Article 9(2)(b) – processing necessary for the purposes of carrying out obligations and exercising rights in the field of employment and health and safety law
Safety, security, and crime prevention	CCTV footage	Legitimate interests – (for safety, security, and crime prevention purposes)
Maintaining accurate records for emergency response, audits, and investigations	Access records	Legal obligation (health and safety requirements) and Legitimate interests (ensuring site safety and security, maintaining audit trails, investigating incidents, misconduct, or breaches, protecting assets and personnel and managing operational risks)

Thomas Johnstone Ltd does not carry out solely automated decision-making that produces legal or similarly significant effects on individuals in relation to site access.

4. Our Facial Recognition System (CloudPass)

We use the CloudPass facial recognition system for site access control.

CloudPass converts each enrolled individual's facial image into a mathematical template (biometric data), which is securely stored and compared at the point of access.

All biometric data is encrypted, stored on secure UK-based servers, and access is limited to authorised personnel only.

We have carried out a Data Protection Impact Assessment (DPIA) for our use of facial recognition to ensure that the processing is necessary, proportionate, and subject to appropriate safeguarding measures.

Alternative access method: Any individual who does not wish to use biometric authentication may request an alternative site access control method. Alternative arrangements will be provided where reasonably practicable and in accordance with our site safety requirements. If an individual selects an alternative method, it will not affect their employment or contractual duties, but may require some additional time and steps to complete.

5. How Long We Keep Your Data

We will only retain your personal data for as long as reasonably necessary to fulfil the purposes we collected it for, including for the purposes of satisfying any legal, regulatory, tax, accounting or reporting requirements. We may retain your personal data for a longer period in the event of a complaint or if we reasonably believe there is a prospect of litigation in respect to our relationship with you.

To determine the appropriate retention period for personal data, we consider the amount, nature and sensitivity of the personal data, the potential risk of harm from unauthorised use or disclosure of your personal data, the purposes for which we process your personal data and whether we can achieve those purposes through other means, and the applicable legal, regulatory, tax, accounting or other requirements.

6. Who We Share Your Data With

We do not sell or share your data for marketing. We may share information in the following circumstances:

- Service providers – trusted third parties (such as security contractors and site management systems) who process data on our behalf under strict written data processing agreements and only on our instructions.
- Legal requirements – where required by law, regulation, or public authorities.
- Corporate transactions – if Thomas Johnstone Ltd undergoes a merger or acquisition, we will ensure your data remains protected.

All processing is carried out in the UK. If any data transfer outside the UK were to occur, we would ensure appropriate safeguards are in place.

7. How We Protect Your Data

We implement appropriate technical and organisational measures to protect your personal data against unauthorised access, alteration, disclosure, or destruction. These measures include access controls, secure systems, and internal policies and procedures designed to safeguard personal information.

Thomas Johnstone Ltd maintains a data security process which records any data breach within the company to allow us to continually identify and address any issues.

8. Your Rights

Under UK GDPR and the Data Protection Act 2018, you have the following rights in relation to your personal data:

- Right of access – to request a copy of the personal data we hold about you.

- Right to rectification – to request correction of inaccurate or incomplete data.
- Right to erasure – to request deletion of your personal data in certain circumstances.
- Right to restriction – to request that we restrict how we process your data in certain circumstances.
- Right to object – to object to processing where we rely on legitimate interests.
- Right to data portability – where processing is based on contract and carried out by automated means.
- Right to withdraw consent – at any time, where processing is based on consent.

Please note that these rights are not absolute and may be subject to legal or regulatory limitations.

If you wish to exercise any of your rights, or if you believe the information we process about you is incorrect, please contact our Data Protection Officer by email at DPO@tjl.com.

To submit a formal data request, please visit <http://portal.tjl.com/External/> and complete the provided form.

9. Complaints

If you are not satisfied with our response, or believe we are processing your personal data not in accordance with the law, you have the right to lodge a complaint with the Information Commissioner's Office (ICO) at www.ico.org.uk.

You can also contact the ICO by:

Telephone: 0303 123 1113

Post: Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF.

Signed:



Name: David Hadow

Position: Joint Managing Director

Date: 21 August 2026

Signed:



Name: Rod Young

Position: Joint Managing Director

Date: 21 August 2026