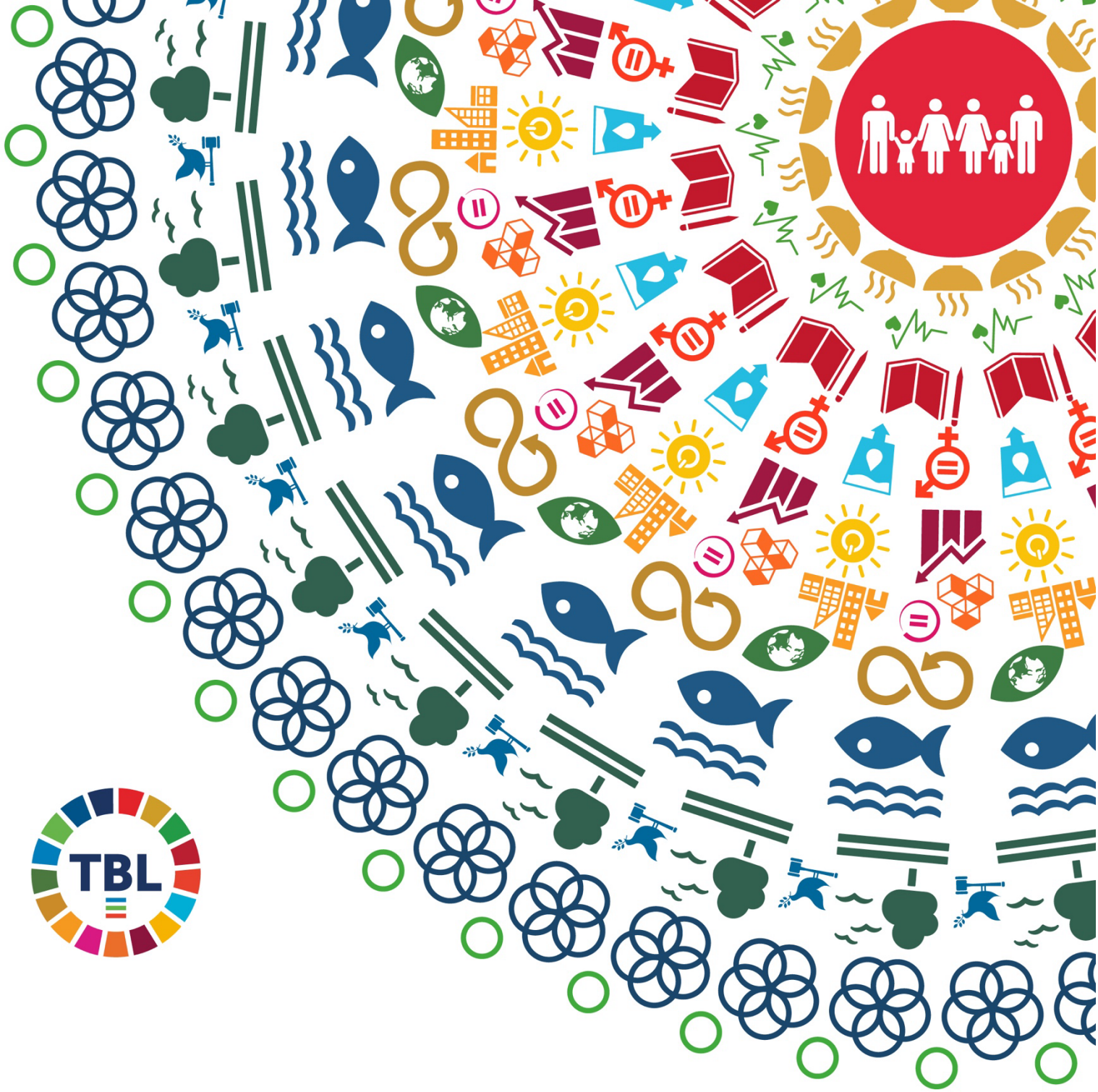




Data Protection Policy

2026

Purpose	3
Scope	3
Key Definitions	3
Roles and Responsibilities	3
Data Protection Principles	3
Lawful bases for using personal information	3
Collecting and using personal information	4
Storage, access, and security	4
Sharing personal information	4
Retention and Deletion.....	5
Individual Rights Requests.....	5
Data Breaches and Reporting	5
Training and compliance	5
Policy Review	5

Purpose

TBL is committed to protecting personal information and handling it lawfully, fairly and securely. This policy explains how we meet our duties under UK data protection law.

Scope

This policy applies to all employees, directors, contractors, and volunteers who handle personal information for TBL. It covers personal information relating to employees, job applicants, customers, suppliers, and other contacts.

Key Definitions

- **Personal information:** information that identifies or relates to an identifiable person.
- **Special category information:** more sensitive information such as health, ethnicity or religious beliefs.
- **Processing:** anything done with personal information, including collecting, storing, using, sharing or deleting.

Roles and Responsibilities

- **Managing Director:** overall accountability for data protection at TBL.
- **Data protection lead (HR):** maintains this policy, advises the business, manages incidents and supports rights requests.
- **All staff:** must follow this policy, complete any training, keep information secure, and report concerns immediately.
- **System owners:** ensure access controls and retention rules are applied in their systems (for example SharePoint, Microsoft 365, Monday.com, Xero, Mailchimp).

Data Protection Principles

TBL will ensure personal information is:

- Used lawfully, fairly, and transparently
- Collected for clear purposes and not used in incompatible ways
- Limited to what is necessary
- Accurate and kept up to date
- Kept only as long as needed
- Kept secure

Lawful bases for using personal information

We only use personal information where we have a lawful basis, such as:

- To perform a contract (for example employment or customer contracts).

- To meet a legal obligation (for example payroll and tax).
- For legitimate business interests (for example running the business, improving services), where those interests do not override individuals' rights.
- With consent where required (for example some marketing).

Special category information will only be used where a valid additional legal condition applies (for example employment, social security and social protection law, or explicit consent where appropriate).

Collecting and using personal information

- We will only collect what we need and will explain why we need it.
- Staff must only access personal information needed for their role.
- Personal information must only be used for the purpose it was collected, unless a lawful reason applies.

Storage, access, and security

TBL uses approved systems to store and manage personal information, including Microsoft 365, Xero, Monday.com and access-controlled SharePoint.

Minimum controls:

- Use SharePoint, Microsoft 365, Xero, and Monday.com as the main storage locations. Do not store work personal information in personal email accounts or personal cloud storage.
- Access is limited on a need-to-know basis and removed promptly when roles change, or someone leaves the company.
- Use strong passwords and multi factor authentication where available.
- Keep devices secured (screen lock, password) and do not leave personal information unattended.
- Do not share personal information via unapproved channels (for example WhatsApp) unless authorised and necessary, and only for low-risk information.
- Follow clear desk and secure disposal practices for printed records.

Sharing personal information

We may share personal information with trusted service providers and professional advisers where necessary. We ensure appropriate written terms are in place where a supplier processes personal information for us.

We may share information where required by law or to protect rights and safety.

International transfers: if a supplier stores or accesses personal information outside the UK, TBL will ensure appropriate safeguards are in place.

Retention and Deletion

TBL will keep personal information only for as long as needed for the purpose it was collected, and in line with legal and business requirements. We will securely delete or destroy information when it is no longer needed.

Individual Rights Requests

People have rights over their personal information including access, correction, deletion (in some cases), restriction, and objection. Requests should be sent to: colin.curtis@tbl-services.com. We will respond within 1 month, subject to identity checks and legal exceptions.

Data Breaches and Reporting

A data breach is any loss, unauthorised access, disclosure, or destruction or personal information.

All suspected or actual breaches must be reported immediately to colin.curtis@tbl-services.com. We will investigate, contain the risk, record the incident, and report to the regulator and affected individuals where required by law.

Training and compliance

All staff will complete data protection training at onboarding and refresh it at least annually. Breaches of this policy may result in disciplinary action.

Policy Review

This policy will be reviewed at least annually and whenever there is a significant change in systems, processing activities, or legal requirements.

Created by	Rachael Davies, Head of People and Business Operations
Date created	January 2024
Date reviewed & revised	March 2025, July 2025, March 2026
Next review due	March 2027

If you have questions, please contact rachael.davies@tbl-services.com



Thank you!

rachael.davies@tbl-services.com

www.tbl-services.com