1. Policy Statement

1.1 This policy details how personal data is collected, handled and stored to meet the Company's data protection standards.

1.2 The purpose of the policy is to:

- Comply with data protection law and good practice
- Protect the rights of workers, customers, suppliers and partners.
- Detail how individual data is processed and stored
- Protect the Company from any risk of data breaches

1.3 This policy should also be read in conjunction with the following Company policies:

- TLC_POL_004_01 Privacy Notice

2. Scope

2.1 This policy applies to all colleagues, temporary colleagues (whether through an agency or direct to TLC Care and Support), colleagues contracted to TLC to undertake work as required and visitors, collectively referred as individuals within this policy.

3. Data Protection Law

3.1 The General Data Protection Regulations (GDPR) which replaces the Data Protection Act 1998 describes how organisations must collect, handle and store personal information. These rules apply regardless of whether data is stored electronically, on paper or on other materials.

3.2 To comply with the law, personal information must be collected and used fairly, stored safely and not disclosed unlawfully.

3.3 The GDPR is underpinned by six principles that personal data must:

- Be processed fairly and lawfully
- Be collected only for specific, lawful purposes
- Be adequate, relevant and limited to what is necessary
- Be accurate and kept up to date
- Not be held for longer than necessary
- Processed in a manner that ensures appropriate security including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage.

3.4 The GDPR includes the following rights for individuals:

- to be informed
- of access
- rectification
- erasure
- restrict processing
- data portability
- to object
- not to be subjected to automated decision-making including profiling.

4. Responsibilities

4.1 All individuals have responsibility to ensure any data collected is stored and handled appropriately and processed in line with GDPR.

4.2 The Data Protection Officer is responsible for:

- Keeping the Company updated about data protection responsibilities and risks
- Reviewing all data protection procedures and related policies
- Handling data protection questions
- Arranging any necessary data protection training
- Identifying what constitutes a potential breach and how to report breaches
- Dealing with requests Data Subject Access Requests (DSAR).

5. General Guidelines

5.1 Individuals are only able to access personal data if a requirement of their work.

5.2 Data should not be shared informally and if access to confidential information is required, individuals must request this from their line managers.

5.3 Individual must keep all data secure, not disclose to unauthorised people, either internally or externally.

5.4 Data should be regularly reviewed and updated if out of date. Data no longer required, should be deleted and disposed of.

5.5 The duration for which data will be retained and deleted in accordance with retention periods.

6. Consent

6.1 The Company will provide every individual access to TLC_POL_005 Privacy Notice.

7. Special Category Data

7.1 The Company may also collect, store and more sensitive personal information called special category data:

- Race or ethnicity, religious beliefs and sexual orientation
- Health, including any medical condition, health and sickness records
- Criminal convictions and offences

7.2 The Company will only use personal information when the law allows. Most commonly, in the following circumstances:

- to perform the contractual obligations
- to comply with a legal obligation

7.3 Where it is necessary for legitimate interests (or those of a third party) and individual interests and fundamental rights do not override those interests.

8. Data Storage

8.1 Data stored either on paper or electronically should be kept in a secure place where unauthorised individuals do not have access.

- When not required, papers or files should be kept in a locked drawer or filing cabinet.
- Papers and printouts should not be left where unauthorised individuals can access.
- Data printouts should be disposed of securely when no longer required.

8.2 Electronic data must be protected from unauthorised access, accidental deletion and malicious hacking attempts.

- Data should be protected by strong passwords and never shared between individuals.
- The use of removable media will only be approved for legitimate business reason and will require a Company issued encrypted USB from IT.
- Data should only be stored on designated drivers and servers and never be saved directly to laptops or other mobile devices such as tablets or smart phones.
- All servers and computers containing data should be protected by approved security software and a firewall and will back up frequently

9. Data Accuracy

9.1 The Company are required to take reasonable steps to keep data accurate and up to date.

- Data will be held in approve central locations. Individuals must not create duplicate or additional data sets.
- Individuals must update personal data as soon as this changes
- The company will update the information held on individuals
- Data should be updated as inaccuracies are discovered

10. Data Subject Access Requests

10.1 Requesting information is called a data subject access request (DSAR).

10.2 All individuals are able to:

- Ask what information the company holds on 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

10.3 DSARs must be in writing/email and identity verification maybe required before the release of data is provided.

10.4 Data will be provided within one calendar month.

11. Data Sharing

11.1 The Company may share individual data with third parties, including third-party service providers and other entities in the group. Third parties will respect the security of individual data and to treat it in accordance with the law

11.2 Personal information may be transferred outside the EU. Similar degree of protection can be expected with personal information.

11.3 The Company may share personal information with third parties where required by law, where it is necessary to administer the working relationship or where there is legitimate interest in doing so.

11.4 Third-party service providers includes: contractors, designated agents and other entities within the Company group.

11.5 The following activities are carried out by third-party service providers: payroll, pension administration, benefits provision and administration, IT services, medical and drug and alcohol screening.

11.6 All third-party service providers and other entities in the group are required to take appropriate security measures to protect personal information in line with the Company policies. Third-party service providers are not permitted to use personal data for their own purposes only to process personal data for specified purposes and in accordance with the Companies instructions.

12. Data Breaches

12.1 The Company policy has processes and procedures in place to mitigate data breaches. In the unlikely event of a data breach this policy will ensure the following:

- Data breach events are detected, reported, categorised and monitored consistently
- Incidents are assessed and responded to appropriately
- Action is taken to reduce the impact of disclosure
- Mitigation improvements are made to prevent recurrence
- Serious breaches are reported to the Information Commissioner's Office (ICO).
- Lessons learnt are communicated to the organisation as appropriate to prevent future incidents.

13. Incident Management

13.1 A data breach is the result of an event or series of events where Personally Identifiable Information (PII) is exposed to unauthorised or inappropriate processing that results the security being compromised.

13.2 The extent of damage or potential damage caused will be determined by the volume, sensitivity and exposure of the PII.

13.3 Breach management aims to detect, report and contain incidents and implement further controls to prevent any recurrence. A log of incidents will be maintained to review trends and identify improvements to reduce the recurrence.

13.4 The Company will implement measures to ensure that data protection breaches are reported and guidelines are issued on how to report breaches for analysis, categorisation and response.

13.5 On discovery of a breach the following steps will be followed:

- Discovery
- Identify
- Assess
- Investigate

- Recommendations

14. Policy Monitoring

14.1 This policy is not contractual and can be amended or withdrawn at any time.

14.2 This policy supersedes any previous agreements and/or documents previously communicated.

14.3 The policy will be monitored to confirm that the above arrangements are being adhered to in all areas.

Revision Date	Reason for Revision	Revised By	Approved By
01/11/2021	Annual Review	Michelle Morgan	