

1. Policy Statement

- 1.1 The Company is committed to protecting the privacy and security of personal information.
- 1.2 This privacy notice describes how the Company collect and use personal information during and after the working relationship, in accordance with the General Data Protection Regulation (GDPR).

2. Scope

- 2.1 This policy applies to all colleagues, temporary workers (whether through an agency or direct), individuals contracted to TLC to undertake works as required and visitors to TLC. (Collectively referred to as individuals in this statement).

3. Data Protection Principles

- 3.1 The Company is a data controller. This means that the Company are responsible for deciding how to hold and use personal information. The Company are required under data protection legislation to notify individuals the information contained within this privacy notice.
- 3.2 The Company will comply with data protection law. This says that the personal information the company hold about individuals must be:
 - Used lawfully, fairly and in a transparent way.
 - Collected only for valid purposes that have been clearly explained and not used in any way that is incompatible with those purposes.
 - Relevant and limited to the purposes advised
 - Accurate and kept up to date.
 - Kept only as long as necessary for the purposes already informed.
 - Kept securely.

4. The Information held

- 4.1 Personal data or personal information means any information about an individual from which that person can be identified. It does not include data where the identity has been removed (anonymous data).
- 4.2 The Company may collect, store, and use the following categories of personal information:
 - Personal contact details such as name, title, addresses, telephone numbers, email addresses
 - Date of birth
 - Gender
 - Marital status
 - Next of kin and emergency contact information
 - National Insurance number
 - Bank account details, payroll records and tax status information
 - Salary, annual leave, pension and benefits information
 - Start date
 - Location of employment or workplace
 - Copy of driving licence
 - Recruitment information (including copies of right to work documentation, references and other information included in a CV, Application Form or cover letter or as part of the application process)

- Employment records (including job titles, work history, working hours, training records and professional memberships)
- Performance information
- Disciplinary and grievance information
- CCTV, and other information obtained through electronic means such as time and attendance systems.
- Photographs

4.3 The Company may also collect, store and use the following special categories of more sensitive personal information:

- Race or ethnicity, religious beliefs and sexual orientation
- Health, including any medical condition, health and sickness records.
- Vaccinations records such as Covid or Flu
- Criminal convictions and offences.

5. How Personal Information is Collected

5.1 The Company typically collect personal information about employees, workers and contactors through the application and recruitment process, either directly from candidates or sometimes from an employment agency. Additional information can be collected from third parties including former employers, credit reference agencies or other background check agencies.

5.2 Additional personal information is collected in the course of job-related activities throughout an employment period.

6. How the Information is used

6.1 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

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

6.3 Personal information in the following situations are likely to be rare:

- To protect individual interests (or someone else's interests).
- Public interest or for official purposes

6.4 Contractual Obligations

- Decisions regarding recruitment or appointments
- Determining the terms and conditions of employment
- Provision of any benefits such as pension or EAP
- Administering the terms and conditions of employment
- Conducting performance reviews.
- Decisions regarding remuneration and compensation.
- Assessing qualifications
- Gathering evidence for possible grievance or disciplinary hearings.
- Education, training and development requirements.
- Ascertaining fitness to work.
- Managing sickness absence.

- Monitoring information and communication systems to ensure compliance with IT policies.
- Conducting data analytics studies to review and better understand employee retention and attrition rates.
- Recording and distribution to interested third parties, of phone conversations made on Company mobiles as dictated by the contract with the client.
- Sponsor and sub-sponsor requests from legitimate third parties

6.5 Legal Obligations

- Checking legally entitlements to work in the UK.
- Paying salaries and deducting tax and National Insurance contributions if applicable.
- Checking eligibility to drive Company Vehicles with DVLA and Insurance providers
- Dealing with legal disputes including accidents at work.
- Complying with health and safety obligations.
- To prevent fraud.
- To ensure network and information security, including preventing unauthorised access to computer and electronic communications systems and preventing malicious software distribution.
- Equal opportunities monitoring.

6.6 Legitimate Interests

- Tender submissions in order to secure additional work
- Business management and planning, including accounting and auditing.

Some of the above grounds for processing will overlap and there may be several grounds which justify the use of personal information.

7. Failing to Provide Personal Information

7.1 Failure to provide certain information when requested, may mean the Company are unable to fulfil its contractual obligations (such as paying salary or providing a benefit). This may prevent the Company from complying with the legal obligations (such as to ensure the health and safety of work force).

8. Change of Purpose

8.1 The Company will only use personal information for the purposes for which it was collected it. Unless it is considered for another reason and that reason is compatible with the original purpose.

8.2 If the Company need to use personal information for an unrelated purpose, individuals will be notified and explained the legal basis in doing so.

8.3 The Company may process personal information without individuals knowledge or consent, where this is required or permitted by law.

9. Sensitive Personal information

9.1 Special categories of particularly sensitive personal information requires a higher levels of protection and may require further justification for collecting, storing and usage.

9.2 Information can be used in the following circumstances and with explicit written consent:

- Where the Company need to carry out legal obligations and in line with data protection policy
- Where it is needed in the public interest, such as for equal opportunities monitoring

- Where it is needed to assess individual working capacity on health grounds, subject to appropriate confidentiality safeguards.

9.3 The Company may process this type of information where it is required for legal claims. Where required to protect individual interests (or someone else's interests) and individuals are not capable of giving consent, or where individuals have already made the information public.

9.4 The Company may also process such information about members or former members in the course of legitimate business activities with the appropriate safeguards.

10. Employer Obligations

10.1 The Company will use particularly sensitive personal information in the following ways:

- Absence, sickness absence or family related leave
- Physical or mental health or disability status, to assess fitness to work and health and safety compliance.
- Race or ethnic origin, religious, philosophical or moral beliefs or sexual orientation, to ensure meaningful equal opportunity monitoring and reporting.

11. Consent

11.1 The Company do not need consent if using special categories of personal information in accordance with the company policy to carry out legal obligations or exercise specific rights in the field of employment law.

11.2 The Company may approach individuals for written consent to process certain particularly sensitive data. Full details will be provided of the information required and the reason.

12. Criminal Convictions

12.1 The Company will collect information about criminal convictions if it is appropriate given the nature of the role and where legally able to do so.

12.2 Where appropriate, information about criminal convictions will be collected as part of the recruitment process or where notified by individuals during the course of working for the Company.

13. Automated decision-making

13.1 Automated decision-making takes place when an electronic system uses personal information to make a decision without human intervention. Automated decision-making is used in the following circumstances:

- Where the Company have notified individuals of the decision and given 21 days to request a reconsideration
- Where it is necessary to perform the contract and the appropriate measures are in place to safeguard individual rights
- In limited circumstances, with explicit written consent and where appropriate measures are in place to safeguard rights

13.2 If the Company make an automated decision on the basis of any particularly sensitive personal information, the Company must have either explicit written consent or it must be justified in the public interest and have in place the appropriate measures to safeguard rights.

13.3 Individuals will not be subject to decisions that will have a significant impact based solely on automated decision-making, unless the Company have a lawful basis for doing so and have notified individuals.

13.4 The Company do not envisage that any decisions will be taken using automated means. However, individuals will be notified in writing if this position changes.

14. Data Sharing

14.1 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

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

14.3 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.

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

14.5 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.

14.6 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.

15. Other Third Parties

15.1 The Company may share personal information with other third parties, for example in the context of the possible sale or restructuring of the business.

15.2 Individual personal information may be shared with a regulator or to otherwise comply with the law.

16. Data Security

16.1 The Company have put in place appropriate security measures to prevent personal information from being lost, used or accessed in an unauthorised way, altered or disclosed.

16.2 The Company access to personal information to only employees, agents, contractors and other third parties who have a business need to know. Personal information will only be processed on authorisation and subject to confidentiality.

16.3 The Company put in place procedures to deal with any suspected data security breach and will notify individuals and any applicable regulator of a suspected breach where legally required to do so.

17. Data Retention

- 17.1 The Company will only retain personal information for as long as necessary to fulfil the purposes it was collected it for, including for the purposes of satisfying any legal, accounting, or reporting requirements.
- 17.2 In some circumstances the Company may anonymise personal information so that it can no longer be associated with individuals, in which case the Company may use such information without further notification to individuals.
- 17.3 Once an individual is no longer an employee, worker or contractor, the Company will retain and securely destroy personal information in accordance with applicable laws and regulations.

18. Rights of Access, Correction, Erasure and Restriction

- 18.1 It is important that the personal information the Company hold is accurate and current. Therefore, individuals are required to inform the Company of any changes.

19. Rights in connection with personal information

- 19.1 **Request access** commonly known as a data subject access request (DSAR). Individuals can request to receive a copy of the personal information held.
- 19.2 **Request correction.** Individuals can have any incomplete or inaccurate information held corrected.
- 19.3 **Request erasure.** Individuals can ask for personal information to be deleted or removed where there is no good reason for the Company continuing to process it. Individuals can ask the Company to delete or remove personal information where individuals have exercised their right to object to processing.
- 19.4 **Object to processing** where the Company are relying on a legitimate interest (or those of a third party) and there is something about an individual's situation which makes an individual object to processing on this ground. Individuals can object to processing personal information for direct marketing purposes.
- 19.5 **Request the restriction of processing.** Individuals can ask the Company to suspend the processing of personal information to establish the accuracy or the reason for processing it.
- 19.6 **Request the transfer** to another party.
- 19.7 If individuals want to review, verify, correct or request erasure of personal information, object to the processing or request the transfer of personal information to another party, please contact the HR Department in writing.

20. Administration Fee

- 20.1 Individuals will not have to pay a fee to access their personal information (or to exercise any of the other rights). However, the Company may charge a reasonable fee if requests for access is clearly unfounded or excessive. Alternatively, the Company may refuse to comply with the request in such circumstances.

21. Identification

- 21.1 The Company may need to request specific information from individuals to confirm identity and ensure access to the right the information (or to exercise any of your other rights).

22. Withdraw Consent

- 22.1 In the limited circumstances where individuals may have provided consent to the collection, processing and transferring of personal information for a specific purpose, individuals have the right to withdraw consent for that specific processing at any time.
- 22.2 To withdraw consent, please contact the People and Culture Team on HR@tlccarehomes.co.uk. Upon receipt of a request to withdrawn consent, the Company will no longer process personal information for the purpose originally agreed to, unless there is another legitimate or legal reason for doing so.

23. Data Protection Officer

- 23.1 The Company have appointed a Data Protection Officer to oversee compliance with the privacy notice.
- 23.2 Any questions about The Company privacy notice or personal information is managed, please contact the DPO.
- 23.3 Individuals have the right to make a complaint at any time to the Information Commissioner's Office (ICO), the UK supervisory authority for data protection issues.

24. Policy Monitoring

- 24.1 This policy is not contractual and can be amended or withdrawn at any time.
- 24.2 This policy supersedes any previous agreements and/or documents previously communicated.
- 24.3 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 Update	Michelle Morgan	