# VERIFICATION OF ACCESSIBLE RECORDS & DATA PROTECTION POLICY

## Policy Statement

London Teachers Supply is fully committed to and compliant with the requirements of the General Data Protection Act 2018 (GDPR), Privacy & Electronic Communications (EC Directive) Regulations 2003 (PECR) and the Conduct of Employment Agencies and Employment Businesses Regulations 2003. The company will therefore follow procedures that aim to ensure that all individuals who have access to any Personal Data held by or on behalf of the company are fully aware of and abide by their duties and responsibilities under the above Act and regulations.

London Teachers Supply regards the lawful and correct treatment of Personal Data as essential to its successful operations and to maintaining confidence between the company, its employees, clients and temporary workers. The company will therefore ensure that it treats Personal Data lawfully and correctly. To this end the company fully endorses and adheres to the Principles of Data Protection as set out in the General Data Protection Regulations 2018 as detailed below.

London Teachers Supply is registered in the register of data controllers with the Information Commissioner's Office (registration number ZB 344193) and this registration is renewed on an annual basis.

We have a detailed Data Protection and Privacy Policy and also have and maintain a valid and current Cyber Essentials Plus Certificate which demonstrates how we guard against cyber threats including but not limited to:

- Operating a secure internet connection.
- Ensuring devices and software have security provision.
- Controlling access to our data and services.
- Protecting our equipment and software from viruses and other malware.
- Keeping our devices and software up to date.

## Scope of the Policy

In order to operate efficiently, London Teachers Supply has to collect and use information about the people with whom it works.

Personal Data must be handled and dealt with properly however it is collected, recorded and used, and whether it be on paper, in computer records or recorded by any other means, and there are safeguards within the GDPR to ensure this.

All employees are required to comply with this policy when dealing with other employees, temporary or agency staff, consultants, work seekers, clients, suppliers, customers and contacts of the Company, and anyone else with whom they come into contact during the course of their employment.

All employees are made fully aware of this policy and of their duties and responsibilities under the GDPR. In addition, we have a full GDPR Data Protection Policy which provides more detailed information relating to our obligations and controls to manage data in line with current legislation.

## Responsibilities

It is the direct responsibility of the Compliance Manager to ensure the implementation of this policy on a day-to-day basis; however, all employees have a responsibility to accept their personal involvement in applying it and must be familiar with the policy and ensure that it is followed by both themselves and employees for whom they have a responsibility.

Disciplinary action may be taken against any employee who acts in breach of this policy. Disciplinary action may include summary dismissal in the case of a serious breach of this policy or repeated breaches. In other cases, it may include a verbal or written warning. Such action will be taken in accordance with the Company's disciplinary procedure.

Breaches of this policy may also result in the employee responsible being held personally liable for compensation if legal action is taken in relation to data protection.

## The Principles of Data Protection

We adhere to the principles relating to Processing of Personal Data set out in the GDPR which require Personal Data to be:

1. Processed lawfully, fairly and in a transparent manner (Lawfulness, Fairness and Transparency).
2. Collected only for specified, explicit and legitimate purposes (Purpose Limitation).
3. Adequate, relevant and limited to what is necessary in relation to the purposes for which it is Processed (Data Minimisation).
4. Accurate and where necessary kept up to date (Accuracy).
5. Not kept in a form which permits identification of Data Subjects for longer than is necessary for the purposes for which the data is Processed (Storage Limitation).
6. Processed in a manner that ensures its security using appropriate technical and organisational measures to protect against unauthorised or unlawful Processing and against accidental loss, destruction or damage (Security, Integrity and Confidentiality).
7. Not transferred to another country without appropriate safeguards being in place (Transfer Limitation).

8. Made available to Data Subjects and Data Subjects allowed to exercise certain rights in relation to their Personal Data (Data Subject's Rights and Requests).

We are responsible for and can demonstrate on request compliance with the data protection principles listed above.

## Lawfulness, Fairness & Transparency

Personal Data must be processed lawfully, fairly and in a transparent manner in relation to the Data Subject.

We will only collect, Process and share Personal Data fairly and lawfully and for specified purposes. The GDPR restricts our actions regarding Personal Data to specified lawful purposes. These restrictions are not intended to prevent Processing but ensure that we Process Personal Data fairly and without adversely affecting the Data Subject. The GDPR allows Processing for specific purposes, some of which are set out below:

- The Data Subject has given his / her Consent;
- The Processing is necessary for the performance of a contract with the Data Subject;
- To meet our legal compliance obligations.;
- To protect the Data Subject's vital interests; or
- To pursue our legitimate interests for purposes where they are not overridden because the Processing prejudices the interests or fundamental rights and freedoms of Data Subjects. The purposes for which we process Personal Data for legitimate interests are set out in our Privacy Policy.

You must identify and document the legal ground being relied on for each Processing activity.

## Consent

A Data Subject Consents to Processing of their Personal Data if they indicate agreement clearly either by a statement or positive action to the Processing. Consent requires affirmative action so silence, pre-ticked boxes or inactivity are insufficient. If Consent is given in a document which deals with other matters, then the Consent must be kept separate from those other matters. For example, we currently request a candidate's Consent when they sign up with us to receive notifications around potential jobs and for us to provide job seeking services.

Data Subjects can easily withdraw Consent to Processing at any time and withdrawal must be promptly honoured. Consent may need to be refreshed if we intend to Process Personal Data for a different and incompatible purpose which was not disclosed when the Data Subject first Consented.

Unless we can rely on another legal basis of Processing, Explicit Consent is usually required for Processing Sensitive Personal Data, for Automated Decision-Making and for cross border data transfers.

Usually we will be relying on another legal basis (and not require Explicit Consent) to Process most types of Sensitive Data. Where Explicit Consent is required, we will issue a Fair Processing Notice to the Data Subject to capture Explicit Consent. Sensitive Personal Data may be particularly relevant when collecting personal and work information from a candidate or temporary worker, therefore, we will take particular care whenever collecting and Processing such information.

We keep records of all Consents so that we can demonstrate compliance with Consent requirements if required to do so.

## Transparency (Notifying Data Subjects)

The GDPR requires us to provide detailed, specific information to Data Subjects and we do this via our Privacy Policy which is accessible on our website.

Whenever we collect Personal Data directly from Data Subjects, we will specify how and why we will use, Process, disclose, protect and retain that Personal Data

## Purpose Limitation

Personal Data will only be collected for specified, explicit and legitimate purposes. It must not be further processed in any manner incompatible with those purposes. We will not use Personal Data for new, different or incompatible purposes from that disclosed when it was first obtained unless we have informed the Data Subject of the new purposes and they have consented where necessary.

## Data Minimisation

Personal Data must be adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed. We will only Process Personal Data when performing when it is required to perform our job duties and services. We will not collect excessive data and we will ensure that when Personal Data is no longer needed for the specified purposes, it is deleted or anonymised in accordance with the Company's data retention guidelines.

## Accuracy

Personal Data must be accurate and, where necessary, kept up to date. It must be corrected or deleted without delay when found to be inaccurate. We will check the accuracy of any Personal Data at the point of collection and at regular intervals afterwards and take all reasonable steps to destroy or amend inaccurate or out-of-date Personal Data.

## Storage Limitation

Personal Data must not be kept in an identifiable form for longer than is necessary for the purposes for which the data is processed. We maintain a retention procedure to ensure Personal Data is deleted after a reasonable time for the purposes for which it was being held, unless a law requires such data to be kept for a minimum time. Thereafter we will take all reasonable steps to destroy or erase it from our systems.

## Data Retention and Disposal

We will retain Personal Data for a reasonable duration to provide a Candidate or worker with our services, or support our Company Personnel, as follows:

| Type of Records | Statutory Retention Period | Statutory Authority |
|---|---|---|
| Accident book / accident records & reports | 3 years from date of the last entry (or if the accident involves a child, until that person reaches the age of 21. | Reporting of Injuries, Diseases and Dangerous Occurrences Regulations 1995 (RIDDOR) (SI 1995/3163) as amended, and Limitation Act 1980. |
| Accounting records | 3 years<br>[this is 6 years for public limited companies] | Section 221 of the Companies Act 1985 modified by the Companies Acts 1989 and 2006. |
| Income tax and NI returns, income tax records and correspondence with HMRC | Not less than 3 years after the end of the financial year to which they relate. | The Income Tax (Employments) Regulations 1993 (SI 1993/744) as amended, for example by The Income Tax (Employments) (Amendment No. 6) Regulations 1996 (SI 1996/2631). |
| Statutory maternity pay records, calculations, certificates or other medical evidence | 3 years after the end of the tax years in which the maternity period ends. | The Statutory Maternity Pay (General) Regulations 1986 (SI 1986/1960) as amended. |
| Wage / salary records, overtime, bonuses, expenses | 6 years | Taxes Management Act 1970. |
| National minimum wage records | 3 years after the end of the pay reference period following the one that the records cover. | National Minimum Wage Act 1998 |
| Records relating to working | 2 years from the date on | The Working Time |

| | | |
|---|---|---|
| time | which they were made | Regulations 1998 (SI 1998/1833). |

For many types of HR records, there is no definitive retention period and we are required to consider carefully how long to keep them. We have based our records retention periods below on the time limits for potential UK tribunal or civil claims and guidance in the Conduct of Employment Agencies and Employment Businesses Regulations 2003. The UK Limitation Act 1980 contains a 6-year time limit for starting many legal proceedings, so where documents may be relevant to a contractual claim, we will keep these records for at least this period. Other records may be retained longer or permanently. These retention periods are in line with CIPD recommendations.

| **Type of Records** | **Minimum Retention Period** |
|---|---|
| Actuarial valuation reports | Permanently |
| Application forms and interview notes (for unsuccessful candidates) | 6-12 months |
| Assessments under health and safety regulations and records of consultations with safety representatives and committees | Permanently |
| Inland Revenue/HMRC approvals | Permanently |
| Parental leave | 5 years from birth/adoption of the child or 18 years if the child receives a disability allowance. |
| Pension scheme investment policies | 12 years from the ending of any benefit payable under the policy. |
| Candidate files, personnel files and training records (including disciplinary records and working time records) | 7 years after the date on which we last provide services to the associated applicant or client or 7 years after employment has ended. We may hold data longer if contractually required to do so, and for contract clients we will hold all data relating to service provided for a minimum of 7 years after the contract expires. Where such records could be relevant to a claim for personal injury, we will retain them for a minimum of 21 years from contract expiry. |
| Redundancy details, calculations of payments, refunds, notification to the Secretary of State | 6 years from the date of redundancy |
| Senior executives' records (that is, those on a senior management team or their | Permanently |

| | |
|---|---|
| equivalents) | |
| Statutory Sick Pay records, calculations, certificates, self-certificates | 6 years after the employment ceases. |
| Timesheets | 2 years after audit |

## Disposal of Records

Electronic records will be securely and permanently deleted as appropriate and London Teachers Supply has facilities for the secure disposal of documentation relating to work seekers, employees and clients.

We will maintain records of disposal and will detail the date and the name of the person who authorised the record's disposal for all records that are either deleted or destroyed.

## Confidentiality

Our staff are provided with instructions relating to confidentiality during induction, as part of their contract and in the staff handbook. This instructs them to:

- Ensure confidential information is stored securely.
- No disclose confidential information without explicit written Consent from the disclosing party.
- Notify the disclosing party if unauthorised access, copying or use of the information is suspected.

Confidential information is disclosed to our staff on a "need to know" basis to enable us to meet our obligations under our contractual frameworks.

## Compliance with the Conduct of Employment Agencies and Employment Businesses Regulations 2003 – Regulation 29

In line with the "Conduct Regulations" London Teachers Supply will store candidate and client data for:

- At least one year after its creation (unless the data is in respect of applications which London Teachers Supply takes no action); and
- At least one year after the date on which we last provide services to the applicant or client to whom it relates.

We may hold data significantly longer if contractually required and for NHS contracts will hold all data relating to work seekers, assignments and clients for a minimum of 7 years after the

contract expires. Where such records could be relevant to a claim for personal injury, we will retain them for a minimum of 21 years from contract expiry.

All data is stored securely on our electronic systems which are password protected with periodic mandatory password changes. Where an employee leaves the business, their passwords and computer access is closed down immediately.

All candidate data is readily accessible on our system and held in a format that can be reproduced in legible form and can be provided on request by the end of the second business day from the date or request by a Contracting Authority or Framework Awarding Body.

We obtain and store the following information from all work seekers:

- Date the application was received.
- The work seeker's name, address and, if under 22 years of age, their date of birth.
- Any terms which apply or will apply between London Teachers Supply and the work seeker, and any document recording any variation thereto.
- Details of the work seeker's training, experience, qualifications, and any authorisation to undertake particular work (and copies of any documentary evidence of the same).
- The names of any clients to whom the work-seeker is introduced or supplied.
- Details of any resulting engagement and the date from which it takes effect (including all assignment start and end dates).
- Details of any requirements specified by the work seeker in relation to taking up employment.
- Names of hirers to whom the work seeker is introduced or supplied.
- Details of any resulting engagement and date from which it takes effect.
- A copy of any contract between the work seeker and any hirer entered into by the agency on the work seeker's behalf.
- Dates of requests of fees from work-seekers and receipts for such fees with copy statements or invoices, numbers and amounts (please note we do not charge fees to work-seekers for our services).
- Details about the work seeker and the position concerned with copies of all relevant documents and dates they were received or sent as the case may be. These include:
    - The ID of the work seeker.
    - The experience, training, qualifications and professional registrations.
    - References.
    - Confirmation that the work seeker is willing to work in the position that they are being submitted for.
    - All relevant pre-employment checks.
    - Health & safety risks.

- Any information received by the agency to indicate that the work seeker is unsuitable for the work being provided.

We are not required to retain details of any work-seeker that we do not provide services to.

Under current data protection laws, Data Subjects (in this case work-seekers) have a right to request that we delete their Personal Data. However, this is not an absolute right - where we have another legal basis to continue to process that data, (e.g. we have a legal obligation to hold certain records for a certain period of time), and those obligations will take precedence over the Data Subject's right.

We are also obliged to obtain and store the following information about hirers (including all relevant documents and dates of receipt) as a minimum:

- The date that the vacancy was submitted.
- Hirers name, address and location of employment.
- Position(s) to be filled.
- Duration of assignment.
- Experience, training, ability, qualifications, professional memberships etc required in respect of the position(s) to be filled.
- Terms & conditions between the hirer and the agency and any documents that detail variations to these.
- Name of work seekers supplied or introduced.
- Details of the engagement and assignment dates.
- Details of fees, pricing and payment including copies of statements and invoices and the date these were requested.

## Use of Cookies & Similar Technologies

A cookie is a small text file that is downloaded onto 'terminal equipment' (e.g. a computer or smartphone) when the user accesses a website. It allows the website to recognise that user's device and store some information about the user's preferences or past actions.

In line with regulation 6 of the PECR, when people visit our website, we:

- Tell people the cookies are there;
- Explain what the cookies are doing and why; and
- Get the person's Consent to store a cookie on their device.

We then allow them to set their preferences to accept or reject cookies by obtaining Explicit Consent. Restricting or rejecting cookies on our website may, however, mean that certain areas of the site will not function correctly.

This is done the first time we set cookies for each piece of equipment and again if we make significant changes to the cookies on the site.

We may also use third-party apps, tools, plug-ins and widgets on our website and these may use automated means to collect information relating to how you interact with these features. Such information collected is subject to the privacy policies of those providers and to applicable law. London Teachers Supply is not responsible for the practices of these providers.

## Access by Data Subjects

Data Subjects have rights when it comes to how we handle their Personal Data. These include rights to:

- Withdraw Consent to Processing at any time (where the Company is relying on Consent);
- Receive certain information about our Processing activities;
- Request access to their Personal Data that we hold;
- Prevent our use of their Personal Data for direct marketing purposes;
- Ask us to erase Personal Data if it is no longer necessary in relation to the purposes for which it was collected or Processed or to rectify inaccurate data or to complete incomplete data;
- Restrict Processing in specific circumstances;
- Challenge Processing which has been justified on the basis of our legitimate interests or in the public interest;
- Request a copy of an agreement under which Personal Data is transferred outside of the EEA;
- Prevent Processing that is likely to cause damage or distress to the Data Subject or anyone else;
- Be notified of a Personal Data Breach which is likely to result in high risk to their rights and freedoms;
- Make a complaint to the supervisory authority; and
- In limited circumstances, receive or ask for their Personal Data to be transferred to a third party in a structured, commonly used and machine-readable format.

We will verify the identity of an individual requesting data under any of the rights listed above and will not allow third parties to persuade us to disclose Personal Data without proper authorisation.

Any Data Subject request must be forwarded to the Operations Manager.

## Right of Audit

London Teachers Supply operates many contracts where we are obliged to provide access

to client and candidate information for quality and audit purposes. Work seekers will be asked to sign a GDPR data protection disclaimer on their application form to give us permission to share their Personal Data with clients and any external auditors as required to support audits.

## Implementation

The Compliance Manager will be responsible for ensuring that the Policy is implemented. Implementation will be led and monitored by the Compliance Manager who will have overall responsibility for:

- The provision of cascade data protection training, for staff within the company.
- For the development of best practice guidelines.
- Carrying out compliance checks to ensure adherence with the General Data Protection Regulations and Conduct of Employment Businesses and Employment Agencies Regulations.

## Review

This policy will be reviewed regularly and may be altered from time to time in light of legislative changes or other prevailing circumstances.