



TDL & HSL Employee Privacy Notice

Data controller: The Doctors Laboratory (TDL) & Health Services Laboratories (HSL), herein known as 'the organisation'.

The organisation collects and processes personal data relating to its employees to manage the employment relationship. The organisation is committed to being transparent about how it collects and uses this data whilst complying with our data protection obligations.

What information does the organisation collect?

The organisation collects and processes a range of information about you. This includes:

- your name, address and contact details, including email address and telephone number, date of birth and gender;
- the terms and conditions of your employment;
- details of your qualifications, skills, experience and employment history, including start and end dates, with previous employers and with the organisation and usually a copy of your CV & Application form;
- information about your remuneration, including entitlement to benefits such as pensions or insurance cover;
- details of your bank account and National Insurance number;
- information about your marital status, next of kin, dependants and emergency contact details;
- information about your nationality and entitlement to work in the UK;
- information about your criminal record;
- details of your schedule (days of work and working hours) and attendance at work;
- details of periods of leave taken by you, including holiday, sickness absence, family leave and sabbaticals, and the reasons for the leave;
- details of any disciplinary or grievance procedures in which you have been involved, including any warnings issued to you and related correspondence;
- assessments of your performance, including appraisals, performance reviews and ratings, training you have participated in, performance improvement plans and related correspondence;
- information about medical or health conditions, including whether or not you have a disability for which the organisation needs to make reasonable adjustments;
- details of trade union membership; and

- equal opportunities monitoring information, including information about your ethnic origin, sexual orientation, health and religion or belief.

The organisation collects this information in a variety of ways. For example, data is collected through application forms, CVs or resumes; obtained from your passport or other identity documents such as your driving licence; from forms completed by you at the start of or during employment (such as benefit nomination forms); from correspondence with you; or through interviews, meetings or other assessments.

In some cases, the organisation collects personal data about you from third parties, such as references supplied by former employers.

Data is stored in a range of different places, including in your personnel file, in the organisation's HR management systems and in other IT systems (including the HR database, Totara and the organisation's email system).

Why does the organisation process personal data?

The organisation needs to process data to enter into an employment contract with you and to meet its obligations under your employment contract. For example, it needs to process your data to provide you with an employment contract, to pay you in accordance with your employment contract and to administer benefit, pension and insurance entitlements.

In some cases, the organisation needs to process data to ensure that it is complying with its legal obligations. For example, it is required to check an employee's entitlement to work in the UK, to deduct tax, to comply with health and safety laws and to enable employees to take periods of leave to which they are entitled.

In other cases, the organisation has a legitimate interest in processing personal data before, during and after the end of the employment relationship.

Processing employee data allows the organisation to:

- run recruitment and promotion processes;
- maintain accurate and up-to-date employment records and contact details (including details of who to contact in the event of an emergency), and records of employee contractual and statutory rights;
- operate and keep a record of disciplinary and grievance processes, to ensure acceptable conduct within the workplace;
- operate and keep a record of employee performance and related processes, to plan for career development, and for succession planning and workforce management purposes;

- operate and keep a record of absence and absence management procedures, to allow effective workforce management and ensure that employees are receiving the pay or other benefits to which they are entitled;
- obtain occupational health advice, to ensure that it complies with duties in relation to individuals with disabilities, meet its obligations under health and safety law, and ensure that employees are receiving the pay or other benefits to which they are entitled;
- operate and keep a record of other types of leave (including maternity, paternity, adoption, parental and shared parental leave), to allow effective workforce management, to ensure that the organisation complies with duties in relation to leave entitlement, and to ensure that employees are receiving the pay or other benefits to which they are entitled;
- ensure effective general HR and business administration;
- provide references on request for current or former employees;
- respond to and defend against legal claims; and
- maintain and promote equality in the workplace.

Where the organisation relies on legitimate interests as a reason for processing data, it has considered whether or not those interests are overridden by the rights and freedoms of employees or workers and has concluded that they are not.

Some special categories of personal data, such as information about health or medical conditions, is processed to comply with industry required standards and carry out employment law obligations (such as those in relation to employees with disabilities and for health and safety purposes).

Information about trade union membership is processed to allow the organisation to deduct correctly for membership through payroll.

Where the organisation processes other special categories of personal data, such as information about ethnic origin, health or religion or belief, this is done for the purposes of equal opportunities monitoring. Data that the organisation uses for these purposes is anonymised or is collected with the express consent of employees, which can be withdrawn at any time.

Employees are entirely free to decide whether or not to provide such data and there are no consequences of failing to do so.

Who has access to data?

Your information may be shared internally, including with members of the HR and Payroll team, your line manager, managers in the business area in which you work and IT staff if access to the data is necessary for performance of their roles.

The organisation shares some aspects of your data with third parties in order to obtain pre-employment references from other employers.

The organisation also shares your data with third parties that process data on its behalf, in connection with payroll, HR database, the provision of training, the provision of benefits and the provision of occupational health services.

For the purpose of investigating any potential legal claims against the organisation, your information may be shared with our insurers in order to obtain insurance advice and services.

The organisation's HR system processes the data held on our employees. Our system provider is ADP who are headquartered in the United States. We do however; have a strict code of confidentiality & clauses in contracts that ensures compliance with the General Data Processing Regulation and Data Protection standards. Some anonymised employee data is also shared with our parent organisation 'Sonic Healthcare', who are based in Australia.

How does the organisation protect data?

The organisation takes the security of your data seriously. The organisation has internal policies and controls in place to try to ensure that your data is not lost, accidentally destroyed, misused or disclosed, and is not accessed except by its employees in the performance of their duties.

Where the organisation engages third parties to process personal data on its behalf, they do so on the basis of written instructions, are under a duty of confidentiality and are obliged to implement appropriate technical and organisational measures to ensure the security of data.

For how long does the organisation keep data?

The organisation will hold your personal data for the duration of your employment. The periods for which your data is held after the end of employment are detailed in our Data Retention Policy, which can be accessed here: <http://www.hslpathology.com/retention-policy/>.

Your rights

As a data subject, you have a number of rights. You can:

- access and obtain a copy of your data on request;
- require the organisation to change incorrect or incomplete data;
- require the organisation to delete or stop processing your data, for example where the data is no longer necessary for the purposes of processing;
- object to processing of your data where the organisation is relying on its legitimate interests as the legal ground for processing when there is good reason to protect your personal data which overrides those legitimate interests;
- ask the organisation to stop processing data for a period of time if data is inaccurate.

If you would like to exercise any of these rights, please contact the Human Resources Department on HR@tdlpathology.com (For subject access requests email to: HRdata@tdlpathology.com).

Whilst all reasonable requests must be considered and addressed, some requests might not be possible to fulfil, such as the deletion of information that we are legitimately obliged to retain for legal reasons.

If you believe that the organisation has not complied with your data protection rights then you should raise your concern(s) with your Line Manager, a member of HR or the Companies Data Controller, in the first instance. Alternatively, you may wish to pursue your concern formally via the Company's grievance procedure.

If you are not satisfied with the action taken following the above then you can complain to the Information Commissioner.

What if you do not provide personal data?

You have obligations under your employment contract to provide the organisation with data. In particular, you are required to report absences from work and may be required to provide information about disciplinary or other matters under the implied duty of good faith. You will also have to provide the organisation with data in order to exercise your statutory rights, such as in relation to statutory leave entitlements. Failing to provide the data may mean that you are unable to exercise your statutory rights.

Certain information, such as contact details, your right to work in the UK and payment details, must be provided to enable the organisation to enter a contract of employment with you. If you do not provide other information, this will hinder the organisation's ability to administer the rights and obligations arising as a result of the employment relationship efficiently.

Automated decision-making

Employment decisions are not based solely on automated decision-making processes.

This notice can be amended by the organisation from time to time and the latest version will be published on organisation's websites.

I hereby confirm that I have read, understood and accept the above information contained herein the Employee Privacy Notice.

.....
XXXX

Date: