St. Peter's Out of School Care Limited

Confidentiality/Privacy Policy

This policy applies to clients, current and former employees, workers and contractors.

Data Protection Principles
The COMPANY will comply with data protection law in relation to clients and employees. This says that the personal information we hold about you must be:

- Used lawfully, fairly and in a transparent way.
- Collected only for valid purposes that we have clearly explained to you and not used in any way that is incompatible with those purposes.
- Relevant to the purposes we have told you about and limited only to those purposes.
- Accurate and kept up to date.
- Kept only as long as necessary for the purposes we have told you about.
- Kept securely.

We may collect, store, and use the following categories of personal information about you:

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). The company collects and processes personal data relating to its employees to manage the employment relationship. The company is committed to being transparent about how it collects and uses that data and to meeting its data protection obligations.

There are "special categories" of more **sensitive personal data** which require a higher level of protection.

What information does the company collect?
The company collects and processes a range of information about clients and employees. This includes:

- Individual name, address and contact details, including email address and telephone number, date of birth and gender for clients and employee's;
- Contact and medical information for clients and employee's
- Details of the level and duration of service for clients
- The terms and conditions of employee's employment;
- Details of employee's qualifications, skills, experience and employment history, including start and end dates, with previous employers and with the company;
- Information about employee's remuneration, including entitlement to benefits such as pensions or insurance cover;
- Details of employees and clients bank accounts
- Details of employee's national insurance and pay numbers

- Information about your marital status, next of kin, dependants and emergency contacts;
- Information about your nationality and entitlement to work in the UK;
- Details of employee's schedule (assignments, days of work and working hours) and attendance at work;
- Details of periods of leave taken by employee's, including holiday, sickness absence, family leave and the reasons for the leave;
- Details of any disciplinary or grievance procedures in which employees have been involved, including any warnings issued to you and related correspondence;
- Assessments of your performance, including appraisals, performance reviews, performance improvement plans and related correspondence;
- Correspondence and other documentation relating to client services and employment matters.

The company may also collect, store and use the following "special categories" of more sensitive personal information for employees including:

- information about medical or health conditions, including whether or not you have a disability for which the company needs to make reasonable adjustments; and
- equal opportunities monitoring information, including information about your ethnic origin, sexual orientation, health and religion or belief.
- Biometric data, including fingerprints, hand geometry and samples.

How is your personal information collected?

The company may collect this information in a variety of ways. For example, for employee's data might be collected through application forms, CVs; 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; from correspondence with you; or through interviews, meetings or other assessments. For clients the information may be requested at the point that a request is made to receive the services the company offers or during the delivery of the service.

In some cases, the company may collect personal data about employees from third parties, such as references supplied by former employers and information from employment background check providers.

Data will be stored in a range of different places, including in client records and employee's personnel files, in the organisation's Payroll and HR management system, and in other IT systems (including the company's email system).

Why does the company process personal data?
The company needs to process data to enter into an employment relationship with employee's and to meet its obligations under an employment contract. For example, it needs to process data to provide employees with an employment contract, to pay them in accordance with the employment terms and conditions and to administer entitlements [benefit, pension etc.].

In some cases, the company 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:

- where we need to protect employees interests (or someone else's interests);
- where it is needed in the public interest (or for official purposes).

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

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

Where the company processes other special categories of personal data, such as information about ethnic origin, sexual orientation, health or religion or belief, this is done for the purposes of equal opportunities monitoring. Data that the company uses for these purposes is anonymised. Employees are entirely free to decide whether or not to provide such data and there are no consequences of failing to do so.

If you fail to provide personal information

If an employee chooses not to or fails to provide certain information when requested, the company may not be able to perform aspects of the contract it has entered into with an employee (such as paying them or providing a benefit), or it may be prevented from complying with our legal obligations (such as to ensure the health and safety of our workers).

Change of purpose

We will only use clients or employee's personal information for the purposes for which we collected it, unless we reasonably consider that we need to use it for another reason and that reason is compatible with the original purpose. If we need to use personal information for an unrelated purpose, we will notify you and we will explain the legal basis which allows us to do so. The company may process personal information without knowledge or consent, in compliance with the above rules, where this is required or permitted by law.

Who has access to data?

Information may be shared internally, including with contractors members of the Support Team (including payroll), a line manager, managers in the business area in which you work, HR Consultants and Legal Advisors and IT staff if access to the data is necessary for performance of their roles and where required by law. The company shares your data with third parties in order to obtain pre-employment references from other employers and to obtain employment background checks from third-party providers. The company may also share your data with third parties in the context of a sale of some or all of its business. In those circumstances the data will be subject to confidentiality arrangements. The company also shares your data with third parties that process data on its behalf, in connection with payroll, the provision of benefits and the provision of occupational health services. We will also share data where there is a legal requirement to do so, for example where TUPE may apply.

We do not allow our third-party service providers to use your personal data for their own purposes. We only permit them to process your personal data for specified purposes and in accordance with our instructions.

The company will not transfer your data to countries outside the European Economic Area.

How does the company protect data?

The company takes the security of your data seriously. The company 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. This includes:

- An Internet facing firewall to prevent outside penetration of the company's records. Policies allow mail to be delivered into the mail server from a specific set of addresses (our external spam filter) but no other access is allowed. This firewall also maintains a list that prevents access to malicious sites on the internet.
- Spam filtering. All our mail passes through a spam filter (BT internet) which looks for unsolicited mail, malicious software and dangerous links.
- Local firewalling. All our machines are individually protected by firewalls. This prevents problem software proliferating through the network and unauthorised access from one machine to another e.g. only the IT provider can remotely connect to a Company laptop.
- Local anti-virus to prevent any malicious software getting through the firewall or spam filters or be brought in by other means. Every machine in the Company has anti-virus software installed which is constantly updated via a server on the network. This software also maintains a web blacklist to prevent access to malicious sites whilst used at the operational settings.
- File access controls. Access to data on the servers is controlled based on need. Management authority is required before any changes of access are made.
- Additional controls. The HR systems, Payroll system are also controlled as above.
- Filing cabinets. Data kept in employee's personnel files are stored in lockable cabinets and secured in a restricted office.
- IT Policy. This policy is to ensure that all information technology users within the company comply with rules and guidelines related to the security of the information stored digitally at any point in the network or within the company's boundaries of authority.
- Social Media Policy. This policy is aimed to educate employees and minimise risks when using social media which can impact the company and employees. Employees are discouraged from social media contacts with clients outside the work operational setting

Where the company engages third parties to process personal data on its behalf, they do so on the basis of written instructions; these parties 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 company keep data?

The company will hold client personal data for the duration of their contractual relationship with the company. When either party ends this relationship personal data is destroyed. Employee personal data is held for the duration of the employment. At the end of employment data will not be kept longer than necessary for the purpose for which it was processed. For example, personal information of employees, including terms and conditions of employment, disciplinary records, reviews and annual leave records will be kept for 7 years after employment ends. The company or its support team will keep hold of employees' PAYE, Payroll records for 7 years after employment ends given the relevance to any pay disputes and as HMRC may request to see them in this time. Occupational Health records will be kept in a suitable form for a minimum of 40 years after the date of last entry.

Rights and duty to inform the company of changes

It is important that the personal information held is accurate and current. Please keep the company informed if personal information changes during the working relationship with the company. Under certain circumstances, by law you have the right to:

- access and obtain a copy of your data on request;
- require the company to change incorrect or incomplete data;
- require the company to delete or stop processing your data, for example where the data is no longer necessary for the purposes of processing; and
- object to the processing of your data where the company is relying on its legitimate interests as the legal ground for processing.
- Request the transfer of your personal information to another party.

If any individual would like to exercise any of these rights, please contact the Manager. If you believe that the company has not complied with your data protection rights, you can complain to the Information Commissioner.

What if you do not provide personal data?

Individuals have some obligations under an employment contract to provide the company with data. In particular, a requirement to report absences or unavailability for a work assignment and may be required to provide information about disciplinary or other matters under the implied duty of good faith. Individuals may also have to provide the company with data in order to exercise their statutory rights, such as in relation to statutory leave entitlements (where these relate to operational periods). Failing to provide the data may mean that individuals may be unable to exercise your statutory rights.

Certain information for employee's, such as contact details, your right to work in the

UK and payment details, have to be provided to enable the company to enter a contract of employment. If individuals do not provide other information, this will hinder the company'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.

The company will regularly review this Confidentiality/Privacy Policy to ensure it remains accurate and up to date.