DATA PROTECTION POLICY

The Company collects, uses and stores certain types of information about its employees, customers, clients and stakeholders to satisfy operational and legal obligations. This personal information must be collected dealt with and stored appropriately, in compliance with the Company's legal obligations under the General Data Protection Regulation (GDPR).

Any employee breach of this policy will be taken seriously and may result in disciplinary action.

Purpose

The Company is fully committed to comply with the GDPR as it applies to all organisations that process data relating to their employees, customers, contractors and clients. It sets out principles which should be followed by those who process data; it gives new and extended rights to those whose data is being processed. To this end, the Company endorses fully and adheres to the key principles of data protection, as set out in Article 5 of GDPR.

- data must be processed lawfully, fairly and in a transparent manner in relation to individuals.
- data must be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.
- data must be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
- data must be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure
- that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.
- data must be kept in a form that permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.
- data must be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

The Data Protection Principles

These principles must be followed at all times when processing or using personal information. Therefore, through appropriate management and strict application of criteria and controls, the Company will:

- observe fully the conditions regarding the fair collection and use of information including the giving of consent
- meet its legal obligations to specify the purposes for which information is used
- collect and process appropriate information only to the extent that it is needed to fulfil its operational needs or to comply with any legal requirements
- ensure the quality of information used
- ensure that the information is held for no longer than is necessary
- ensure that the rights of people about whom information is held can be fully exercised under the GDPR (ie the right to be informed that processing is being undertaken, to access one's personal information; to prevent processing in certain circumstances, and to correct, rectify, block or erase information that is regarded as incorrect)
- take appropriate technical and organisational security measures to safeguard personal information
- publicise and abide by individuals' right to appeal or complain to the supervisory authority (the Information Commissioner's Office (ICO)) in the event that agreement cannot be reached in a dispute regarding data protection
- ensure that personal information is not transferred abroad without suitable safeguards.

Status of this policy
The policy does not form part of the formal contract of employment Company employees but it is a condition of employment that employees will abide by the rules and policies made by the Company from time to time. Any failure to follow the Data Protection Policy may lead, therefore, to disciplinary proceedings. This policy will be monitored and reviewed to ensure that it is compliant with the GDPR and other relevant legislation and the Company may amend this policy accordingly.

Employee responsibilities
All employees are responsible for:

- checking that any information that you provide to the Company in connection with your employment/engagement is accurate and up to date;
- informing the Company of any changes to information which you have provided, e.g. changes of address;
- if and when, as part of your duties, you collect personal data about other people (for example in your capacity as a manager)
- you must comply with the principles set out in this policy. If you are unsure or feel you require training in relation to GDPR principles, please contact the Data Controller;
- you may have access to the personal data of other individuals (and of customers and clients) in the course of your employment, contract, volunteer period, internship or apprenticeship. Where this is the case, the Company requires you to help meet its data protection obligations to staff, customers and clients.

Individuals who have access to personal data are required:

- to access only data that they have authority to access and only for authorised purposes;
- not to disclose personal data either orally or in writing or via Web pages or by any other means, accidentally or otherwise except to individuals (whether inside or outside the Company) who have appropriate authorisation;
- unauthorized disclosure will usually be a disciplinary matter and may be considered gross misconduct in some cases;
- to keep data secure (for example by complying with rules on access to premises, computer access, including password protection, and secure file storage and destruction);
- not to remove personal data, or devices containing or that can be used to access personal data, from the Company's premises without adopting appropriate security measures (such as encryption or password protection) to secure the data and the device; and
- not to store personal data on local drives or on personal devices that are used for work purposes.

Failing to comply with these obligations may amount to a disciplinary offence, which will be dealt with under the Company's disciplinary procedure. Significant or deliberate breaches of this policy, such as accessing employee or customer data without authorisation or a legitimate reason to do so, may constitute gross misconduct and could lead to dismissal without notice.

Employee personal data
The Company is committed to being transparent about how it collects and uses personal data collected about you and to meeting its data protection obligations in this regard. Full information is set out in the Employee Privacy Notice in compliance with GPDR, a copy of which is made available to all employees.

You are responsible for:

- checking that any information that you provide to the Company in connection with your employment is accurate and up to date

- informing the Company of any changes to information that you have provided, e.g. changes of address, either at the time of appointment or subsequently. The Company cannot be held responsible for any errors unless the employee has informed it of such changes.

Enforcement of the policy
If you consider that this policy has not been followed in respect of Personal Information about you, you should raise the matter initially with the Data Controller, Phillip Wilcox-Moore.

If the matter is not resolved by the Data Controller, you should escalate your concern by raising a grievance under the Grievance Procedure.

If you are concerned that the correct policies are not being followed with regard to other peoples' personal data, you should make your concerns known to the Data Controller or the appropriate authority in accordance with the Whistleblowing Policy.

Training
The Company will provide training to all individuals about their data protection responsibilities as part of the induction process (and at regular intervals thereafter). Individuals whose roles require regular access to personal data, or who are responsible for implementing this policy or responding to subject access requests under this policy, will receive additional training to help them understand their responsibilities.

Subject Consent
The GDPR sets a high standard for consent and requires a positive opt-in. Neither pre-ticked boxes nor any other method of default consent are allowed. As required by the GDPR, asks for separate consent for separate items and will not use vague or blanket requests for consent. As well as keeping evidence of any consent, the Company ensures that people can easily withdraw consent (and tells them how this can be done).

It should be noted, however, that consent is only one of the lawful bases on which data processing depends. In brief, the others include the following:

- Contract: if processing someone's personal data is necessary to fulfil the Company's contractual obligations to them (eg to provide a quote).
- Legal obligation: if processing personal data is necessary to comply with a common law or statutory obligation.
- Vital interests: not one that will occur often as it refers to processing personal data to protect someone's life (and even then, it cannot be relied on with regard to health data or other special category data if the individual is capable of giving consent).
- Legitimate interests: the most flexible lawful basis for processing and one which applies when data is used in ways people would reasonably expect and which have a minimal privacy impact, or where there is a compelling justification for the processing.
- Note that the GDPR provides for special protection for children's personal data and the Company will comply with the requirement to obtain parental or guardian consent for any data processing activity involving anyone under the age of 16.

Subject access requests
Individuals have the right to make a subject access request. If an individual makes a subject access request, the Company
will tell them:

- whether or not their data is processed and if so why, the categories of personal data concerned and the source of the data if it is not collected from the individual;
- to whom their data is or may be disclosed, including to recipients located outside the European Economic Area (EEA) and the safeguards that apply to such transfers;
- for how long their personal data is stored (or how that period is decided);
- their rights to rectification or erasure of data, or to restrict or object to processing;
- the right to data portability
- the right to compensation for any damage/distress suffered from any breach;
- their right to complain to the Information Commissioner if they think the Company has failed to comply with their data protection rights; and
- whether or not the Company carries out automated decision-making and the logic involved in any such decision making.

The Company will also provide the individual with a copy of the personal data undergoing processing. This will normally be in electronic form if the individual has made a request electronically, unless he/she agrees otherwise.

Any subject access request should be sent to the Company's Data Controller, Phillip Wilcox-Moore, email: pwilcox.moore@axterltd.co.uk. In some cases, the Company will inform the individual if they need to verify their identity for the request to be processed.

The Company will normally respond to a request within a period of one month from the date it is received. In some cases, such as where the Company processes large amounts of the individual's data, it may respond within three months of the date the request is received. The Company will write to the individual within one month of receiving the original request to tell him/her if this is the case.

25.25 If a subject access request is manifestly unfounded or excessive, the Company is not obliged to comply with it. A subject access request is likely to be manifestly unfounded or excessive where it repeats a request to which the Company has already responded. If an individual submits a request that is unfounded or excessive, the Company will notify them that this is the case and whether or not it will respond to it.

Other rights
Individuals have a number of other rights in relation to their personal data. They can require the Company to:

- rectify inaccurate data;
- stop processing or erase data that is no longer necessary for the purposes of processing;
- stop processing or erase data if the individual's interests override the Company's legitimate grounds for processing data (where the Company relies on its legitimate interests as a reason for processing data);
- stop processing or erase data if processing is unlawful;
- stop processing data for a period if data is inaccurate or if there is a dispute about whether or not the individual's interests override the Company's legitimate grounds for processing data;
- to ask the Company to take any of these steps, a request should be sent to Phillip Wilcox-Moore, email: pwilcox.moore@axterltd.co.uk.

International data transfers
The data that we collect from you may be transferred to, and stored at, a destination outside the European Economic Area ("EEA"). We are committed to ensuring that adequate safeguards are in place when transferring Personal Data outside the EEA. As such, we will take reasonable steps to ensure that your

personal information is adequately protected in accordance with the requirements of UK data protection law.

Any questions or concerns about the interpretation or operation of this policy should be taken up with the Data Controller.

Data security
The Company takes the security of HR-related personal data seriously. The Company has in place procedures and controls to protect personal data against loss, accidental destruction, misuse or disclosure, and to ensure that data is not accessed, except by employees in the proper performance of their duties.

Where the Company engages third parties to process personal data on its behalf, such parties must provide sufficient guarantees to implement appropriate technical and /or company measures to ensure the protection of the rights of the individual.

Data breaches
If the Company discovers that there has been a breach of personal data that poses a risk to the rights and freedoms of individuals, it will report it to the Information Commissioner within 72 hours of discovery. The Company will record all data breaches regardless of their effect.

If the breach is likely to result in a high risk to the rights and freedoms of individuals, the Company will tell affected individuals that there has been a breach and provide them with information about its likely consequences and the mitigation measures it has taken.

If the Company has not already communicated the personal data breach to the individuals, the Information Commissioner's Office having considered the likelihood of the personal data breach resulting in a high risk to the rights and freedoms of individuals may decide to do so.

Enquiries
Phillip Wilcox-Moore is the person with responsibility for data protection compliance. Questions about this policy, requests for further information, or an individual's concerns about the operation of this policy in respect of their personal data should be emailed to pwilcox.moore@axterltd.co.uk.

This policy will be monitored and reviewed to ensure that it is compliant with the GDPR and other relevant legislation, and the Company may amend this policy accordingly.

Axt.Int.Data-Protection-Policy_V05_2907202