Strategy IT

Data Protection Policy

Company	Data Protection Officer	Regulations
Strategy IT Limited	Paula Musekiwa - 07939 222 942	Data Protection Act 2018 UK General Data Protection Regulation (UK GDPR)

STATEMENT OF GENERAL INTENT

We need to gather and use certain personal information about individuals, including: employees, customers, suppliers, business contacts and other individuals we have a relationship with or may need to contact. Most of the personal information will have been provided to us by the individual. We aim to keep personal data safe, private and accurate. We are committed to comply with the Data Protection Act 2018 and UK General Data Protection Regulation (UK GDPR). Guided by the Data Protection Principles, we will ensure that personal data is processed fairly, lawfully and in a transparent manner, used only for limited, justifiable business reasons, not disclosed unlawfully, never sold, limited to what is necessary, recorded accurately and kept up to date where necessary, only retained for as long as required and kept safe and secure.

Subject to Review	Signed	Date
Annually	Paula Musekiwa	01 April 2022

RESONSIBILITIES

Company and Directors Key Responsibilities

- Ensure standards in the policy are established and communicated to staff.
- Ensure that the policy is readily available to staff.
- Ensure the policy is published on the website.
- Respect the confidentiality of all personal data.
- Ensure that all employees receive appropriate training on data protection.
- Ensure access to personal data is given only to staff who need it to carry out their duties.
- Provide clarification, where required, to improve staff understanding.
- Assess and monitor compliance with the policy.
- Take appropriate action at the earliest opportunity to manage non-compliance with the standards set out in the policy.
- Actively promote the Company's commitment to data protection.
- Set a positive personal example to staff.

Data Protection Officer Key Responsibilities

- Monitor the implementation of the policy throughout the Company and review its appropriateness annually.
- Investigate complaints or breaches and implement corrective action.
- Arrange data protection training for employees and keep a record of completion.
- Fulfil data subject requests within one calendar month.
- Investigate complaints from data subjects.
- Act as the liaison between the Information Commissioner's Office (ICO) and the Company.
- Review legislation and implement any new requirements pertaining to the Company.
- Liaise with directors and staff as and when appropriate.
- Liaise with contractors, suppliers and other business partners as and when appropriate.

Employees Key Responsibilities

- Familiarise themselves with the policy and fully comply with it.
- Ask for clarification on any aspects of the policy that they are unsure about.
- It is mandatory for all employees to undertake the Company's data protection training.
- Access to personal data should be given only to employees who need it to carry out their duties.
- Personal data should not be shared informally.
- Keep all personal data secure from unauthorised viewings and access.
- Electronically stored personal data should be protected by strong passwords that should never be shared and Multifactor Authentication (MFA) should be used where possible.
- Personal data stored on removable media should be kept locked away when not in use.
- Personal data should not be disclosed to unauthorised people, either within the Company or externally.
- Ensure that personal data is accurately recorded.
- Personal data should be regularly reviewed and updated or deleted (as appropriate) if it is found to be out of date or incorrect.
- If personal data is no longer required, it should be deleted and/or disposed of securely.
- It is an offence for any person to knowingly or recklessly obtain or disclose personal data.
- It is an offence to sell or offer to sell personal data.
- Report, as soon as possible, any known or suspected breach of the policy to the Data Protection Officer.

ARRANGEMENTS	
Personal Data (Personal Information)	Any information relating to an identified or identifiable living individual.
Data Subject (Individual)	The individual whom particular personal data is about.
Processing	Almost anything done with data counts as processing; including collecting, recording, storing, using, analysing, combining, disclosing or deleting it.
Controller	A controller is the organisation, such as the Company, that decides how and why to collect and use the data. The controller must make sure that the processing of that data complies with data protection law.
Processor	A processor is the organisation, such as the Company, who processes data on behalf of the controller and in accordance with their instructions. Processors have some direct legal obligations, but these are more limited than the controller's obligations.
Principles	The Company is committed to comply with the principles set out in the UK GDPR (Article 5) for processing personal data: • **Lawfulness, Fairness and Transparency** – Personal data should be processed lawfully, fairly and in a transparent manner in relation to the data subject. • **Purpose Limitation** – Personal data should only be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes. • **Data Minimisation** – Personal data should be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed. • **Accuracy** – Personal data should 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.

	• **Storage Limitation** – Personal data is to be kept for no longer than is necessary for the purposes for which the personal data are processed. • **Integrity and Confidentiality** – Personal data should 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. • **Accountability** – The Company shall be responsible for, and be able to demonstrate, compliance with the above principles.
Lawful Bases	The lawful bases for processing personal data are set out in the **UK GDPR (Article 6)**. At least one of these should apply whenever personal data is processed by the Company. • **Consent** – The data subject has given clear consent for the Company to process their personal data for a specific purpose. They have the right to withdraw consent at any time. Explicit consent requires a very clear and specific statement of consent - a positive opt-in. Consent requests should be separate from other terms and conditions. • **Contract** – the processing is necessary for a contract the Company have with the individual, or because they have asked the Company to take specific steps before entering into a contract. • **Legal Obligation** – the processing is necessary for the Comapny to comply with the law (not including contractual obligations). • **Vital Interests** – The processing is necessary to protect someone's life. • **Public Task** – the processing is necessary for the Company to perform a task in the public interest or for the Company's official functions, and the task or function has a clear basis in law. • **Legitimate Interests** – the processing is necessary for the individual's legitimate interests or the legitimate interests of a third party, unless there is a good reason to protect the individual's personal data which overrides those legitimate interests. There are three elements to the legitimate interests' basis: o Identify a legitimate interest o Show that the processing is necessary to achieve it o Balance it against the individual's interests, rights and freedoms
Individual Rights (Data Subject Rights)	The **UK GDPR** provides the following rights for data subjects: • **The Right to be Informed** – Individuals have the right to be informed about the collection and use of their personal data. Individuals should be provided with privacy information within a reasonable period of obtaining the data and no later than one calendar month. Privacy information includes: o Purposes for processing their personal data o Retention periods for that personal data o Who it will be shared with

	• **The Right of Access (Subject Access)** – Individuals have the right to access their personal data. • **The Right to Rectification** – Individuals have the right to have inaccurate personal data rectified or completed if it is incomplete. • **The Right of Erasure (The Right to be Forgotten)** – Individuals have the right to have their personal data erased where there is no compelling reason for its continued processing. This request can be declined if the personal data is required for legal or regulatory purposes for example. • **The Right to Restrict Processing** – Individuals have the right to restrict the processing of their personal data where there is no compelling reason for its continued processing. • **The Right to Data Portability** – Individuals have the right to receive personal data they have provided to us (the controller) in a structured, commonly used and machine-readable format. It also gives individuals the right to request that their data be transmitted directly to another data controller. • **The Right to Object** – Individuals have the right to object to the processing of their personal data. The right to object only applies in certain circumstances, whether it applies depends on the purposes and lawful basis for processing. • **Rights in Relation to Automated Decision Making and Profiling** – Automated decision making and profiling can only be carried out where the decision is necessary for the entry into or performance of a contract, authorised by domestic law applicable to the controller or based on the individual's explicit consent.
Types of Personal Data Collected and Processed	The Company currently collect and process the following types of personal data: • Personal contact details such as name, title, addresses, telephone numbers and personal email addresses. • Next of kin and/or emergency contacts. • National Insurance number. • Bank account details, payroll records and tax status information. • Salary, annual leave, pension and benefits information. • Start date and leaving date. • Location of employment or workplace. • Copy of driving licence and passport. • Recruitment information (including copies of right to work documentation, references and other information included in a CV or cover letter or as part of the application process). • Full employment records for (including contract, terms and conditions, job titles, work history, working hours, promotion, absences, attendances, training records and professional memberships). • Performance and appraisal information. • Disciplinary and grievance information. • Surveillance video recordings. • Information about the individual's use of our information and communications systems. • Photographs and videos.

	• Accident book, first aid records and injury at work information.
	• Evidence of rights to work in the UK.
	• Security clearance information.
	• Gender.
	• We will also collect, store and use the following 'special categories' of more sensitive personal information:
	  ○ Information about individual's health, including any medical condition, health and sickness records.
	  ○ Racial or ethnic origin.

How Personal Data is Collected	• Most of the personal data we process is provided to the Company directly by the individual. • We typically collect personal information about employees and contractors through the application process and contract arrangements, either directly from candidates or from an agency. We will sometimes collect additional information from third parties including former employers or other background check agencies. • We will collect additional personal information throughout the period the individual is working for us.

How we Use Personal Data	• We will only use personal information when the law allows us to.
	• Situations in which we will process personal information are listed below:
	  ○ Making a decision about an individual's employment or engagement.
	  ○ Determining the terms on which an individual works for the Company.
	  ○ Checking the individual is legally entitled to work in the UK.
	  ○ Provide the individual with the security clearance appropriate for their role.
	  ○ Paying an individual and, if they are an employee, deducting tax and National Insurance contributions.
	  ○ Liaising with the individual's pension provider, providing information about changes to their employment e.g. promotions, changing in working hours.
	  ○ General administration of the contract the Company have entered into with the individual.
	  ○ Business management and planning, including accounting and auditing.
	  ○ Conducting performance reviews, managing performance and determining performance requirements.
	  ○ Making decisions about salary reviews and compensation.
	  ○ Assessing qualifications for a particular job or task, including decisions about promotions.
	  ○ Gathering evidence and any other steps relating to possible grievance or disciplinary matters and associated hearings.
	  ○ Making decisions about the individual's continued employment or engagement.
	  ○ Making arrangements for the termination of our working relationship.
	  ○ Education, training and development requirements.
	  ○ Dealing with legal disputes involving the individual, or other employees and contractors, including accidents at work.
	  ○ Ascertaining the individual's fitness to work and managing sickness absence.
	  ○ Complying with health and safety obligations.
	  ○ To prevent fraud.

	○ To monitor the individual's business and personal use of our information and communication systems to ensure compliance with our Code of Conduct. ○ Equal opportunities monitoring. • Some of the purposes will overlap and there can be several grounds which justify our use of personal information. • We will only use 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 or new purpose, we will notify the individual and we will explain the legal basis which allows us to do so. • We will if necessary process personal information without the individual's knowledge or consent where this is required or permitted by law.
Sharing Personal Data (Disclosing Personal Data)	• We will share personal information with third parties when: ○ It is necessary to administer the working relationship with an individual. ○ There is substantial public interest to do so. The Data Protection Officer may need to consult with directors and/or legal advisers. ○ Requested by law enforcement agencies, HMRC or other authorities. In such circumstances the Data Protection Officer will ensure the request is legitimate before disclosing the requested data. The Data Protection Officer may need to consult with directors and/or legal advisers. • We expect third parties to respect the security of personal data and to treat it in accordance with the law. • Personal data will never be sold or offered for sale.
Personal Data Storage	**Personal Data Stored on Paper** • Should be kept in a secure place where unauthorised staff or members of the public cannot see it e.g. printouts should not be left on a printer. • When not being used personal data should be kept locked in a drawer or filing cabinet. **Personal Data Stored Electronically** • Should be protected from unauthorised access, accidental deletion and malicious hacking attempts. • Should be protected by strong passwords that should never be shared and Multifactor Authentication (MFA) should be used where possible. • If data is stored on removable media e.g. CD, DVD, USB Stick, these should be encrypted, password protected and kept locked away when not in use. • Data should be backed up frequently. • All servers and computers containing data should be encrypted, protected by security software and a firewall. • Servers containing personal data should be sited in a secure location.
Personal Data Retention and Disposal	• We will only retain personal data for as long as necessary to fulfil the purposes we collected it for, including for the purposes of satisfying any legal, accounting, or reporting requirements. • We keep personal data for six years after the individual's relationship with us ends, unless we are required to keep it longer for legal or regulatory purposes. • We will then securely dispose of personal data by: ○ Shredding paper documents; or ○ Irreversibly deleting electronically stored records.

Exercising Individual Rights (Exercising Data Subject Rights)	• Individuals can exercise their rights verbally or in writing. • Requests should be responded to within one calendar month. • A fee cannot be charged unless the request is manifestly unfounded or excessive. • The Data Protection Officer should be informed of any data subject requests as soon as possible.
Accessing Personal Data	• When working with personal data, staff should ensure that their computer screen cannot be read by unauthorised staff or members of the public. • Staff working with personal data should ensure that their screen is always locked when left unattended. • Personal data should not be shared informally. • Data should be encrypted before being transferred electronically.
Personal Data Accuracy	• Reasonable steps are to be taken to ensure data is kept accurate and up to date. • Data should be held in as few places as necessary. Staff should not create any unnecessary additional data sets. • Staff should take every opportunity to ensure data is updated e.g. confirm customer details when they call. • Data should be updated as inaccuracies are discovered e.g. if a customer can no longer be reached on a stored telephone number, it should be removed from the database.
Individual Complaints	• Individuals have the right to complain if they feel their data has been mishandled. • Individuals are encouraged to complain to the Company in the first instance, but they are entitled to complain directly to the Information Commissioner's Office (ICO). Contact details are provided at the end of the policy. • The Data Protection Officer should be informed of any complaints immediately. • All complaints will be fully investigated by the Company. • We will take appropriate action to prevent, as far as possible, a further occurrence.
Personal Data Breach	• We will notify individuals and any applicable regulator of a suspected breach where we are legally required to do so. • All data breaches will be fully investigated by the Company. • Individuals and staff are encouraged to raise any concerns at the earliest possible stage. • If individuals suspect a breach of the policy has occurred or that it may occur, they must notify the Data Protection Officer or a Director as soon as possible. • We aim to encourage openness and will support anyone who raises genuine concerns in good faith under the policy, even if they turn out to be mistaken. • We are committed to ensuring no one suffers any detrimental treatment as a result of reporting genuine concerns in good faith under the policy. Detrimental treatment includes dismissal, disciplinary action, threats or other unfavourable treatment connected with raising a concern. • All concerns will be fully investigated by the Company. • We will take appropriate action to prevent, as far as possible, a further occurrence.
Staff Complaints and Breaches of the Policy	• Staff are encouraged to raise any concerns at the earliest possible stage. • If staff believe or suspect a breach of the policy has occurred or that it may occur, they must notify the Data Protection Officer or a Director as soon as possible. • We aim to encourage openness and will support anyone who raises genuine concerns in good faith under the policy, even if they turn out to be mistaken. • We are committed to ensuring no one suffers any detrimental treatment as a result of reporting genuine concerns in good faith under the policy. Detrimental treatment includes dismissal, disciplinary action, threats or other unfavourable treatment connected with raising a concern.

	• All concerns will be fully investigated by the Company. • We will take appropriate action to prevent, as far as possible, a further occurrence.

Disciplinary Actions	• Unauthorised disclosure of personal data is a disciplinary matter that may be considered a gross misconduct and could lead to termination of employment.
	• Any staff who breach the policy will be subject to disciplinary action.
	• Disciplinary actions will vary depending on the violation.
	• If we find that an individual or organisation working on our behalf has breached the policy we will take appropriate action.
	• Possible consequences include:
	  ○ Remediation and reprimand
	  ○ Remediation and demotion
	  ○ Suspension or termination of employment
	  ○ Suspension or termination of business relationship
	  ○ Legal action

Review	• The policy will be reviewed annually. • The policy will be reviewed in response to changes in legislation and industry best practice.

COMPANY CONTACTS		
Name	**Position**	**Contact Details**
Robert Musekiwa	Director	Mobile: 07931 121 962 Email: robert.musekiwa@strategyit.co.uk
Paula Musekiwa	Director Data Protection Officer	Mobile: 07939 222 942 Email: paula.musekiwa@strategyit.co.uk

INFORMATION COMMISSIONER'S OFFICE (ICO) CONTACT DETAILS
Address: Information Commissioner's Office Wycliffe House Water Lane Wilmslow Cheshire SK9 5AF Helpline: 0303 123 1113 Website: https://www.ico.org.uk