# DATA PROTECTION POLICY

Introduction

Jam International studies academy hold personal data about our employees, clients, suppliers and other individuals for a variety of business purposes.

This policy sets out how we seek to protect personal data and ensure that staff understand the rules governing their use of personal data to which they have access in the course of their work. In particular, this policy requires staff to ensure that the Data Protection Officer (DPO) be consulted before any significant new data processing activity is initiated to ensure that relevant compliance steps are addressed.

## Definitions

**Business purposes** The purposes for which personal data may be used by us:

Personnel, administrative, financial, regulatory, payroll and business development purposes.

*Business purposes include the following:*

- *Compliance with our legal, regulatory and corporate governance obligations and good practice*
- *Gathering information as part of investigations by regulatory bodies or in connection with legal proceedings or requests*
- *Ensuring business policies are adhered to (such as policies covering email and internet use)*
- *Operational reasons, such as recording transactions, training and quality control, ensuring the confidentiality of commercially sensitive information, security vetting, credit scoring and checking*
- *Investigating complaints*
- *Checking references, ensuring safe working practices, monitoring and managing staff access to systems and facilities and staff absences, administration and assessments*
- *Monitoring staff conduct, disciplinary matters*
- *Marketing our business and improving services*

**Personal data** Information relating to identifiable individuals, such as job applicants, current and former employees, agency, contract and other staff, clients, suppliers and marketing contacts.

*Personal data we gather may include: individuals' contact details, educational background, financial and pay details, details of certificates and diplomas, education and skills, marital status, nationality, job title, and CV.*

**Sensitive personal data** *Personal data about an individual's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership (or non-membership), physical or mental health or condition, criminal offences, or related proceedings—any use of sensitive personal data should be strictly controlled in accordance with this policy.*

## Scope

This policy applies to all staff. You must be familiar with this policy and comply with its terms.

We may supplement or amend this policy by additional policies and guidelines from time to time. Any new or modified policy will be circulated to staff before being adopted.

Who is responsible for this policy?

Priscilla is fulfilling the Data Protection Officer role for the company and has overall responsibility for the day-to-day implementation of this policy

Priscilla is fulfilling the Data Protection Officer role for the company and has overall responsibility for the day-today implementation of this policy.

# Our procedures

Fair and lawful processing

We must process personal data fairly and lawfully in accordance with individuals' rights. Staff training will be provided to ensure that you all know what this means in practise and our processes are designed to maintain company compliance with current personal data protection law and regulation. The Data Protection principles we must follow are: that Personal data shall be:

- Processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency');
- Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ('purpose limitation');
- Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');
- 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 ('accuracy');
- kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('storage limitation');
- 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 ('integrity and confidentiality').

The Data Protection Officer's responsibilities:

The data protection officer shall have at least the following tasks:

- Inform and advise employees who carry out processing of their obligations pursuant to Data Protection Regulation and other relevant data protection provisions.
- To monitor compliance with Data Protection Regulation and the policies of the company in relation to the protection of personal data, including the assignment of responsibilities, awareness-raising and training of staff involved in processing operations, and the related audits;
- To provide advice where requested as regards the data protection impact assessment and monitor its performance.
- To provide the point of contact for the GDPR regulator and data subjects.

Responsibilities of the IT Manager

- To ensure 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 ('integrity and confidentiality').

- The IT Manager should be part of the Data Protection Management Team.

Responsibilities of the Marketing Manager

- Approving data protection statements attached to emails and other marketing copy
- Coordinating with the DPO to ensure all marketing initiatives adhere to data protection laws and the company's Data Protection Policy

Sensitive personal data

In most cases where we process sensitive personal data we will require the data subject's *explicit* consent to do this unless exceptional circumstances apply, for example, where we are required to do this by law. Any such request for consent will need to clearly identify what the data is, why it is being processed and to whom it will be disclosed.

- Accuracy and relevance

We will ensure that any personal data we process is accurate, adequate, relevant and not excessive, given the purpose for which it was obtained. We will not process personal data obtained for one purpose for any unconnected purpose unless the individual concerned has agreed to this or would otherwise reasonably expect this.

Individuals may ask that we correct inaccurate personal data relating to them. If you believe that information is inaccurate you should record the fact that the accuracy of the information is disputed and inform the DPO.

Your personal data

You must take reasonable steps to ensure that personal data we hold about you is accurate and updated as required. For example, if your personal circumstances change, please inform the Data Protection Officer so that they can update your records.

Data security

You must keep personal data secure against loss or misuse. Where other organisations process personal data as a service on our behalf, the DPO will establish what, if any, additional specific data security arrangements need to be implemented in contracts with those third party organisations.

Storing data securely

- In cases when data is stored on printed paper, it should be kept in a secure place where unauthorised personnel cannot access it
- Printed Personal data must not be left unattended or in view and data should be shredded when it is no longer needed. When not in use printed or hard copies of Personal data must be stored in a secure environment.
- Data stored on a computer should be protected by strong passwords (please refer to the information security policy).
- Data stored on CDs or memory sticks must be locked away securely when they are not being used
- The DPO must approve any cloud used to store data
- Servers containing personal data must be kept in a secure location, away from general office space
- Data should be regularly backed up in line with the company's backup procedures
- Data should never be saved directly to mobile devices such as laptops, tablets or smartphones

All servers containing sensitive data must be approved and protected by security software and strong firewall.

Data retention

Personal data may only be retained based on a ‘current’ lawful basis and legitimate purpose. We must retain personal data for no longer than is necessary.

Transferring data internationally

There are restrictions on international transfers of personal data. You must not transfer personal data anywhere outside the UK without first consulting the Data Protection Officer.

# Subject access requests

Please note that under the General Data Protection Regulation, individuals are entitled, subject to certain exceptions, to request access to information held about them.

If you receive a subject access request, you should refer that request immediately to the DPO. We may ask you to help us comply with those requests.

Please contact the Data Protection Officer if you would like to correct or request information that we hold about you. There are also restrictions on the information to which you are entitled under applicable law.

Processing data in accordance with the individual’s rights

- You should abide by any request from an individual not to use their personal data for direct marketing purposes and notify the DPO about any such request.
- Do not send direct marketing material to someone electronically (e.g. via email) unless you have an existing business relationship with them in relation to the services being marketed.
- Please contact the DPO for advice on direct marketing before starting any new direct marketing activity.
- Training
- All staff will receive training on this policy. New joiners will receive training as part of the induction process. Further training will be provided at least every six months or whenever there is a substantial change in the law or our policy and procedure.

Training is provided through an in-house seminar on a regular basis.

It will cover:

- The law relating to data protection
- Our data protection and related policies and procedures.

Completion of training is compulsory.

# GDPR provisions

Where not specified previously in this policy, the following provisions will be in effect on or before 25 May 2018.

## Privacy Notice – transparency of data protection

Being transparent and providing accessible information to individuals about how we will use their personal data is important for our organisation. The following is the information that every privacy notice needs to include:

1. Identity and contact details of the controller, their representative or the Data Protection Officer
2. Purpose and lawful basis for processing
3. Legitimate interests of the controller and third party, where applicable
4. The categories of data held (not required if data came from the subject)
5. Any recipient or categories of recipients of the personal data
6. Details of transfers to third countries and safeguards
7. Retention period or criteria used to determine the retention period of the data
8. The existence of each of the data subjects rights
9. The right to withdraw consent at any time, where relevant
10. The right to lodge a complaint with a supervisory authority
11. The source of the personal data and whether it came from publicly accessible sources (not required if data came from the subject)
12. Whether the personal data is part of a statutory or contractual requirement or obligation and possible consequences of failing to provide the personal data
13. The existence of automated decision making, including profiling, and information about how decisions are made, the significance and the consequence

Conditions for processing

We will ensure any use of personal data is justified using at least one of the lawful conditions for processing and this will be specifically documented. All staff who are responsible for processing personal data will be aware of the conditions for processing. The conditions for processing will be available to data subjects in the form of a privacy notice.

## Justification for personal data

We will process personal data in compliance with all six data protection principles.

We will document the additional justification for the processing of sensitive data.

## Consent

The personal data that we collect is subject to a positive action by the subject, which needs to be documented, to validate that ‘Consent’ is the lawful basis for processing that personal data. Consent can be revoked but the subject at any time.

## Criminal record checks

Any criminal record checks are justified by law. Criminal record checks cannot be undertaken based solely on the consent of the subject.

## Data portability

Upon request, a data subject should have the right to receive a copy of their data in a structured format. These requests should be processed within one month, provided there is no undue burden and it does not compromise the privacy of other individuals. A data subject may also request that their data is transferred directly to another system. This must be done for free.

## Right to be forgotten

A data subject may request that any information held on them is deleted or removed, and any third parties who process or use that data must also comply with the request. An erasure request can only be refused if an exemption applies.

## Privacy by design and default

Privacy by design is an approach to projects that promote privacy and data protection compliance from the start. The DPO will be responsible for conducting Privacy Impact Assessments and ensuring that all IT projects commence with a privacy plan.

## International data transfers

No data may be transferred outside of the EU without first discussing it with the data protection officer.

## Data audit and register

Regular personal data audits to manage and mitigate risks will be conducted using a Data Protection Impact Analysis (DPIA). The DPIA contains information on what data is held, where it is stored, how it is used, who is responsible and any further regulations or retention timescales that may be relevant.

Reporting breaches

All members of staff have an obligation to report actual or potential data protection compliance failures. This allows us to:

- Investigate the failure and take remedial steps if necessary
- Maintain a register of compliance failures
- Notify the Supervisory Authority (SA) of any compliance failures that are material either in their own right or as part of a pattern of failures

Please refer to our Compliance Failure Policy for our reporting procedure.

Monitoring

Everyone must observe this policy. The DPO has overall responsibility for this policy. They will monitor it regularly to make sure it is being adhered to.

# Consequences of failing to comply

We take compliance with this policy very seriously. Failure to comply puts both you and the organisation at risk.

The importance of this policy means that failure to comply with any requirement may lead to disciplinary action under our procedures which may result in dismissal. If you have any questions or concerns about anything in this policy, do not hesitate to contact the DPO.