TRUST ACADEMY

Training...for Excellence!!!

ZIMBABWE PROJECT TRUST

T/A

TRUST ACADEMY

DATA PROTECTION POLICY

2024

Trust Academy collects information from students, employees, suppliers and other stakeholders and treats all the information with strict confidentiality in line with its Data Protection Policy. This policy should therefore be made available to all stakeholders.

1 Purpose

This policy explains how the Trust Academy complies with the Zimbabwe Data Protection Act 2017. The College is committed to being transparent about how it collects and uses the personal data of its students and employees, and to meeting its data protection obligations. This policy sets out the College's commitment to data protection and individual's rights and obligations in relation to personal data.

2 Scope

This policy applies to **all** personal data handled by the College, data held in paper files AND electronically. This policy applies regardless of where the data is held, ie if it is held on personally owned equipment or outside College property.

This policy applies to all College staff, whether permanent, temporary, contractors, consultants and students.

3 Responsibility

The overall responsibility of this Data Protection Policy lies in the College Principal who is the College's Chief Executive Officer

4 Definitions

"Personal data" is any information that relates to an individual who can be identified from that information.

"Processing" is any use that is made of data, including collecting, storing, amending, disclosing or destroying it.

"Special categories of personal data or sensitive personal data" means information about an individual's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health, sex life or sexual orientation, genetics and biometric data.

"Criminal records data" means information about an individual's criminal offences and convictions, and information relating to criminal allegations and proceedings.

5 Data protection principles

The College processes personal data in accordance with the following data protection principles:

- The College processes personal data lawfully, fairly and in a transparent manner.
- The College collects personal data only for specified, explicit and legitimate purposes.
- The College processes personal data only where it is adequate, relevant and limited to what is necessary for the purposes of processing.
- The College keeps accurate and up to date personal data and takes all reasonable steps to ensure that inaccurate or out of date personal data is rectified or deleted without delay.
- The College keeps personal data only for the period necessary for processing.
- The College processes personal data in line with the data subject's rights.
- The College puts in place appropriate security measures to make sure that personal data is secure, and protected against unauthorised access or unlawful processing, and accidental loss, destruction or damage.

6 Legal basis for processing personal or sensitive data

The College will only process **personal data** if it can satisfy at least one of the following conditions in relation to that data:

1. **Consent** – the data subject whom the personal data is about has consented to the processing
2. **Contractual** – processing is necessary for the performance of a contract with the data subject or to take steps to enter into a contract eg for an employment contract
3. **Legal obligation** – processing is necessary for compliance with a legal obligation
4. **Protection of vital interests of a data subject –** where it is necessary to *protect* an interest which is essential *for* the life of the *data subject* or that of another natural person
5. **Public interest/official authority** - processing is necessary for the performance of tasks carried out by a public authority or private organisation acting in the public interest.
6. **Legitimate interests** – processing is necessary for purposes of legitimate interests pursued by the College or a third party, except where such interests are overridden by the interests, rights or freedoms of the data subject.

The College will only process special category data or criminal records where:

- The data subject has given explicit consent to the processing of the personal data for one or more specified purposes. For the consent to be explicit, the data subject must

signify their agreement and there must be some statement or a clear affirmative action that signifies agreement to the processing of personal data relating to them.
- The information is required by law to process the data for employment purposes.
- The information is needed to protect the vital interests of the data subject or another, and consent cannot be given or reasonably sought.

7 Individual Rights

As a data subject, individuals have a number of rights in relation to their personal data.

Subject Access Requests (SAR)

Individuals are entitled to access the information that the College holds about them. This is known as the right of subject access.

If an individual makes a subject access request, the College will comply with the relevant legislation:

- confirm whether any personal data is being processed;
- provide a description of the personal data, the reasons it is being processed, and whether it will be given to any other organisations or people;
- provide a copy of the information comprising the data; and details of the source of the data (where this is available).

This will normally be in electronic form if the individual has made a request electronically, unless they agree otherwise.

8 Information about Examinations

Special rules apply to subject access requests relating to information about the outcome of examinations. These rules apply to requests for examination results, examination scripts or examiners' comments and are designed to prevent the right of subject access being used as a means of circumventing the College's processes for announcing results.

Examination Results

In the case of examination results, the period in which the College has to deal with a request for access is extended if the request is made before the results are announced. The College must respond within:

1. Five months of the date of the request; or
2. 40 days of the date the results are published, whichever is earlier.

Examination scripts – Examination scripts are exempt from disclosure in the event of a subject access request. Therefore, legally the College has no obligation to provide copies for candidates who ask for them. The College adopts a policy that candidates have no automatic right of access to examination scripts, but a candidate attending an official College guidance interview may be given access to scripts in the presence of and at the discretion of, the interviewing examiner.

9 Other Rights

1. Right of access
2. Right to data portability
3. Rights in relation to inaccurate personal or incomplete data
4. Rights to object to or restrict our data processing
5. Rights to erasure
6. Right to withdrawal of consent

10 Data security

The College takes the security of personal data seriously. The College has internal policies and controls in place to protect personal data at rest or in transit against loss, accidental destruction, misuse or disclosure, and to ensure that data is not accessed, except by staff in the proper performance of their duties.

Where the College engages third parties to process personal data on its behalf, such parties do so on the basis of written instructions, ie a data sharing agreement and/or under contractual agreement. Third party suppliers are under a duty of confidentiality and are obliged to implement appropriate technical and organisational measures to ensure the security of data.

11 International data transfers

The College will not transfer personal data to countries outside Zimbabwe unless there are suitable safeguards, and the country or territory can ensure an adequate level of protection of the rights and freedoms of data subjects in relation to the processing of personal data.

12 Roles and Responsibilities

Individual obligations

Students, employees and job applicants are responsible for helping the College keep their personal data accurate and up to date.

Staff may have access to the personal data of other individuals (in the course of their, employment, contract, volunteer period, internship or apprenticeship). Where this is the case, the College relies on individuals to help meet its data protection obligations to staff and to members, customers and clients.

Staff who are processing personal data on behalf of the College are required:

- to only access data that they have authority to access and only for authorised purposes;
- not to disclose data except to individuals (whether inside or outside the College) who have appropriate authorisation;
- to keep data secure (for example by complying with rules on access to premises, computer access, 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 College's premises without adopting appropriate security measures (such as encryption and password protection) to secure the data and the device; and
- not to use personal email addresses to conduct College business.

13 Provision of data to police and other third parties

Specific procedures apply to the provision of data to third parties. Guidance on this is available to staff.

Personal data requests will occasionally be received from the police; requests must be made in writing and must be referred to the Principal (principal@trustacademy.co.zw) for approval. The exemption given to the police to pursue their enforcement functions does not cover the disclosure of all personal information held on an individual. It only allows the College to release personal information for the stated purpose(s) and only if not releasing it would be likely to prejudice legitimate investigations.

If a subject data request is received from an individual after a personal data request has been made by the police, the relevant police force must be consulted before any decision is made to release details of the personal data request to the individual.

In addition, staff must ensure the following in relation to sharing any personal data with a third party:

- When bulk sharing personal data with another organisation, advice is routinely sought from the Principal (or other such contractual arrangement) is in place.
- Where personal or sensitive information is being collected for a new operational purpose, the Principal should always be informed.
- Ensure that all requests for disclosures for personal or sensitive information are sent to the Principal in the first instance.

14 Breach of Policy

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