DEWDROP VOCATIONAL INSTITUTE

POLICIES

& PROCEDURES

Data Management Policy

|  |  |  |
| --- | --- | --- |
| **Title: Data Management Policy** | | |
| **Prepared by:**  Agatha Nnaji | **Reviewed and**  **approved by:** Agatha Nnaji | **Type:**  Policy |
| **Department:** | **Version:** 1 |
| **Effective date:**  January 24, 2022 | **Date updated:**  January 22, 2022 | **Policy Number:**  POL-001 |

**GENERAL INFORMATION**

1. **Data Protection**

The Institute shall comply strictly with the Data Protection Laws of Nigeria. It shall ensure that all sensitive documents pertaining to its training and examination activities are securely stored in a safe, steel cabinet or vault with a lock combination, accessible solely to select and appropriate officials of the Institute, with the pre-approval of the Head of the Institute.

Records are stored in secure safe, steel cabinets, shelves with locks and where necessary, a soft copy is maintained online/off-site with pre-approved multi-levels of authorization and access to the documents.

We rely on the accuracy of information completed by each applicant and contained in the Institute’s application form, as well as the accuracy of other data presented throughout the hiring process and employment. Any misrepresentations, falsifications, or material omissions in any of this information or data may result in exclusion of the individual from further consideration for employment or, if the person has been hired, termination of employment.

It is the responsibility of each Learner or Employee to promptly notify the Institute of any changes in their personal data such as contact address, telephone numbers, names and numbers of dependents, next of kin and qualification details.

Personnel files are the property of Dewdrop Institute and access to the information is restricted. Senior Management staff who have a legitimate reason to review the file of the reports will be allowed to do so. Employees who wish to review their own files should contact the Centre Admin with reasonable notice. Such employee may review his/her personnel file in the presence of a qualified Admin Staff.

The Centre retains the Portfolio of Evidence (PoE) of each Learner in a secure storage when they graduate and will release it to them after the subsequent sampling activity by City & Guilds External Verifier. However, the following assessment records are kept for reference purposes for a period of three years:

* Assessment plans, action plans and feedback reports.
* Candidate interview records.
* Internal verifier (IV) sampling plans, records, and feedback reports.
* Record of achievement/tracking documents.

# Registration

* 1. Applicants' details will be recorded at the point of receipt. All information relating to the data collected in the equality and diversity recruitment monitoring form (Age, gender, race, tribe, religion, sexual orientation) will be hidden from all those involved in the recruitment and selection process. The information collected will be solely used for the purposes of equality monitoring.
  2. All completed application forms are private and confidential

# Computer and Data/Information Security

All resources of the Institute, including computers, email, and voicemail are provided for legitimate use. If there are occasions where it is deemed necessary to examine data beyond that of the normal business activity of the Institute then, at any time and without prior notice, the Institute maintains the right to examine any systems and inspect and review all data recorded in those systems. This will be undertaken by authorized employee only. Any information stored on a computer, whether the information is contained on a hard drive, USB pen or in any other manner may be subject to scrutiny by the Institute. This examination helps ensure compliance with internal policies and the law. It supports the performance of internal investigations and assists in the management of information systems. In line with City & Guilds’ requirements, the Institute will comply with its obligations under the Data Protection Act including the Data Protection Principles

The Institute shall:

* + - issue a unique ID number and user password to each Learner or associate
    - inform its Learners in writing of the Learner Data that it collects and the purposes for which it is collected (which shall include as a minimum the transfer of the Learner Data for the purposes set out in City & Guilds’ Quality Assurance Requirements)
    - obtain the prior written consent of each Learner to the transfer of his/her Learner Data to City & Guilds for the purposes of quality assurance, confirming assessment results, awarding certificates, and informing its regulatory and other relevant industry bodies
    - ensure adequate technical and organizational security measures are in place to prevent unauthorized access to or loss and/or destruction of the data

# The Data Protection Notice

When collecting personal data, the Institute would issue a data protection notice to ensure that its Learners are aware of the data that will be collected and how it will be used. The Institute’s data protection notice allows it to transfer data to City & Guilds:

1. in relation to personal data for the following purposes:
   * To undertake administration in relation to the qualification for which the Learner is registered, including processing, and issuing a certificate on successful completion of the Learner’s qualification or specified units of it.
   * To contact Learners directly in relation to City & Guilds Centre approval or qualification approval and/or quality assurance purposes undertaken by City & Guilds for the qualifications which the Learner is registered for, and investigations into allegations of suspected malpractice.
   * To inform Learners of products or services offered by City & Guilds.
   * To disclose to relevant regulators or for the purposes of apprenticeships to the relevant sector skills Agencies where so required.
2. account for Learners where there is a requirement to do so; and
3. contact a Learner directly if there is a requirement for such bodies and the information is not readily accessible by other means.
4. in relation to sensitive personal data, for the following purposes:
   * To administer requests for reasonable adjustments under the Access of Assessment policy.
   * To carry out statistical analysis (on an anonymized basis) which may be carried out by City & Guilds or selected third parties.
   * To monitor (on an anonymized basis) equal opportunities relating to ethnicity or disability or other such monitoring purposes.

# Data Protection Guidelines 2013 Under Empowerment of National Information Technology Development Agency (NITDA) ACT 2007

Data Protection Guidelines is the guidelines on the processing of information relating to identifiable individual’s Personal Data, including the obtaining, holding, use or disclosure of such information to protect such information from inappropriate access, use, and disclosure.

Personal data is any information relating to an identified or identifiable natural person ("data subject"); information relating to an individual, whether it relates to his or her private, professional, or public life. It can be anything from a name, address, a photo, an email address, bank details, posts on social networking websites, medical information, or a computer’s IP address.

Any information which the Institute holds is potentially disclosable to a requester under one of these pieces of legislation. This includes emails too.

Users need to be sure that they are not breaching any data protection when they write and send emails. This could include but is not limited to:

* Passing on personal information about an individual or third party without their consent.
* Keeping personal information longer than necessary.
* Sending personal information to a party outside the Institute.

Email should where possible be avoided when transmitting personal data about a third party. Any email containing personal information about an individual may be liable to disclosure to that individual under the Data Protection Guideline 2013. This includes comment and opinion, as well as information. Therefore, this should be borne in mind when writing emails, and when keeping them.

When using the Institute’s email, users must:

* Ensure they do not disrupt the Institute’s wider IT systems or cause an increase for significant resource demand in storage, capacity, speed or system performance e.g., by sending large attachment to a large number of internal recipients.
* Ensure they do not harm the Institute’s reputation, bring it into disrepute, incur

liability on the part of DDI, or adversely impact on its image.

* Not seek to gain access to restricted areas of the network or other “hacking activities”

is strictly forbidden

* Must not use email for the creation, retention, or distribution of disruptive or offensive messages, images, materials, or software that include offensive or abusive comments about ethnicity or nationality, gender, disabilities, age, sexual orientation, appearance, religious beliefs and practices, political beliefs, or social background. Employees who receive emails with this content from other employees of the Institute should report the matter to their line manager or supervisor.
* Not send email messages that might reasonably be considered by recipients to be bullying, harassing, abusive, malicious, discriminatory, defamatory, and libelous or contain illegal or offensive material, or foul language.
* Not upload, download, use, retain, distribute, or disseminate any images, text, materials, or software which might reasonably be considered indecent, obscene, pornographic, or illegal.
* Not engage in any activity that is likely to
  + Corrupt or destroy other users’ data or disrupt the work of other users
  + Waste employee effort or Institute resources, or engage in activities that serve to deny service to other users
  + Be outside of the scope of normal work-related duties – for example, unauthorized selling/advertising of goods and services
  + Affect or have the potential to affect the performance of damage or overload the Institute system, network, and/or external communications in any way
  + Be a breach of copyright or license provision with respect to both programs and data, including intellectual property rights
  + not send chain letters or joke emails from an Institute account.

Employees who receive improper email from individuals inside or outside the Institute, should discuss the matter in the first instance with their Head of Centre or Supervisor.

Personal use of the Institute’s email is **not** permitted.

# Penalties for Improper Use

1. *Withdrawal of facilities:* Users in breach of these regulations may have access to Institute IT facilities restricted or withdrawn.
2. *Disciplinary Action:* Breaches of these regulations may be dealt with under the Institute’s disciplinary procedures. It may lead to termination of employment from the Institute.
3. *Breaches of the law:* Where appropriate, breaches of the law will be reported to the police.

***Acknowledgment by the Learner:***

I have received a copy of the above policy which I have read and understood.

Name: …………………………………….

Signature: ………………………………………

Date: ………………………………………