



**NATIONAL EDUCATION TRUST (NET)  
JOB DESCRIPTION**

|                          |                                |
|--------------------------|--------------------------------|
| <b>JOB TITLE:</b>        | <b>Data Protection Officer</b> |
| <b>JOB GRADE:</b>        | <b>Level 4</b>                 |
| <b>POST NUMBER:</b>      | <b>TMP15393SB</b>              |
| <b>DIVISION/UNIT:</b>    | <b>Executive Office</b>        |
| <b>REPORTS TO:</b>       | <b>Executive Director</b>      |
| <b>MANAGES DIRECTLY:</b> | <b>N/A</b>                     |

This document will be used as a management tool and, specifically, will enable the classification of positions and the evaluation of the performance of the post incumbent.

This document is validated as an accurate and true description of the job as signified below:

\_\_\_\_\_  
Employee

\_\_\_\_\_  
Date

\_\_\_\_\_  
Board Chairman

\_\_\_\_\_  
Date

\_\_\_\_\_  
Head of Department/Division/Unit

\_\_\_\_\_  
Date

\_\_\_\_\_  
Human Resource Division MoEY/NET

\_\_\_\_\_  
Date

## **STRATEGIC OBJECTIVES OF THE UNIT:**

- To provide adequate and well-maintained school spaces, enhanced infrastructure and an appropriate teaching environment.
- To be the agency through which Government of Jamaica (GoJ) accesses donations from local, regional and international bodies for the funding of educational development projects.
- To create and foster partnerships with public and private sector organisations as well as the Jamaican Diaspora, which will facilitate opportunities for funding of educational infrastructure and other educational projects.

## **JOB PURPOSE:**

Under the general direction of the Executive Director, the Data Protection Officer is responsible for ensuring that the National Education Trust (NET) operates in accordance with the Data Protection Act 2020. The incumbent is also responsible for providing technical advice and coordinating all aspects relating to data privacy. S/he will play a critical role in safeguarding the privacy rights of individuals for whom data is held or processed by NET and will ensure that sensitive data is protected in accordance with the law.

## **KEY OUTPUTS:**

- External regulations (Data Protection Act) and internal controls adhered to;
- Data Protection framework and strategy developed and implemented;
- Data protection impact assessments conducted;
- Breaches identified and notifications prepared;
- Reports prepared and submitted;
- Continuous monitoring conducted;
- Adherence/compliance with standards monitored;
- Governance and accountability mechanisms evaluated and recommendations made;
- Research and analysis conducted and findings documented;
- Continuous improvement strategies developed and implemented;
- Advice and recommendations provided;

- Sensitization sessions conducted.

## **KEY RESPONSIBILITY AREAS:**

### **Technical / Professional Responsibilities**

- Implement measures and a privacy governance framework to manage data use in compliance with the Data Protection Act, including developing templates for data collection, and assisting with data mapping.
- Ensures that the National Education Trust (NET) processes personal data in compliance with the data protection standards and the Data Protection Act and good practice;
- Consults with the Office of the Information Commissioner (OIC) to resolve any doubt about how the provisions of the Data Protection Act and any Regulations made thereunder are to be applied;
- Ensures that any contravention of the data protection standards or any provisions of the Data Protection Act by NET is dealt with in accordance with the provisions of the Data Protection Act;
- Keeps abreast of Jamaica Data Protection laws and regulations, and industry best practices and international laws including the European Union's General Data Protection Regulations (GDPR), Electronic Privacy Act and other international data protection laws;
- Notifies in writing, the Data Controller of any contravention of the data protection standards or any provisions of the Data Protection Act;
- Investigate and respond to data security breaches or security incidents promptly, ensuring appropriate notices are provided to the regulatory authorities, affected individuals, and other relevant parties as required by law.
- Reports any contravention by NET of the data protection standards or any provisions of the Data Protection Act to the OIC, if the contravention is not rectified within reasonable time after the notification;
- Assists data subjects in the exercise of their rights under the Data Protection Act, in relation to the NET;
- Develops internal policies and procedures related to the processing of personal

data;

- Makes recommendations for the appropriate organisational and technical measures to ensure the security of personal data;
- Serves as the primary contact for the OIC on issues relating to the processing of data, and to consult, where appropriate, with regard to any other matter;
- Develops and implements Standard Operating Procedures (SOPs) for addressing all complaints pertaining to the organisation's privacy policies and procedures;
- Provides advice/information to NET and its employees on their obligations under the Data Protection Act and state data protection provisions;
- Manages and conducts ongoing reviews of NET's Data Protection Framework;
- Disseminates current information on policies, procedures and legislation for NET's staff to be aware as well as to promote the quality culture;
- Develops and implements approved certification mechanisms to exhibit compliance;
- Monitors and evaluates recommendations implemented for addressing weakness and deficiencies in relation to the processing of personal data;
- Prepares reports and presentations on analysis and findings;
- Conducts a data protection Impact Assessment in respect of all personal data in the custody or control of NET;
- Conduct periodic assessments to identify potential risks, gaps, or breaches in data protection and develop strategies to mitigate these risks.
- Conduct sensitization sessions for staff on the components of the Data Protection Act, Regulations and policies;
- Collaborates with the NET's MIS Officer in the maintenance of a data security incident management plan to ensure timely remediation of incidents including impact assessments, security breach response, complaints, claims or notifications and responding to subject access requests;
- Collaborates with the Internal Auditor, Legal Affairs & Company Secretary, and other key stakeholders to monitor, implement and analyse compliance programmes;
- Monitors to ensure that the NET's ICT systems and procedures conform with the relevant data privacy and protection law, regulation and policy;
- Participates in the collection of data, analysis and reports on key performance

measures;

- Provides responses to comments and queries from data subjects in relation to the processing of personal data;
- Provide regular reporting to the Executive Director on data protection activities, compliance status and emerging privacy risks.
- Monitors changes to local privacy laws and makes recommendations where necessary.

### **Other**

Performs any other duty as assigned by the Senior Director,

### **PERFORMANCE STANDARDS:**

- External regulations (Data Protection Act) and internal controls adhered to within accordance with legislative framework;
- Data Protection framework and strategy developed and implemented within accordance with legislative framework;
- Data protection impact assessments conducted within agreed timeframes;
- Breaches identified and notifications prepared within agreed timeframes;
- Reports prepared and submitted within agreed timeframes;
- Continuous monitoring conducted within accordance with legislative framework;
- Adherence/compliance with standards monitored within accordance with legislative framework;
- Governance and accountability mechanisms evaluated and recommendations made;
- Research and analysis conducted and findings documented within accordance with legislative framework;
- Continuous improvement strategies developed and implemented within accordance with legislative framework;
- Technical advice and recommendations provided within agreed timeframes;
- Sensitization sessions conducted within agreed timeframes.

## CONTACTS

### **Internal**

| <b>Contact (Title)</b> | <b>Purpose of Communication</b>                      |
|------------------------|--|
| Executive Director     | To receive and provide guidance and technical advice |
| Unit Heads             | To receive and provide information                   |
| Internal Auditor       | To provide technical advice and guidance             |
| MIS Officer            | To provide technical advice and guidance             |
| All Staff members      | To provide technical advice and guidance             |

### **External**

| <b>Contact (Title)</b>                 | <b>Purpose of Communication</b>   |
|--|---|
| Office of the Information Commissioner | To obtain and share information relating to the administration of the act |
| Stakeholders                           | To receive and provide information  |
| Members of the Public                  | To receive and provide information  |

## REQUIRED COMPETENCIES:

### **Core**

- Excellent oral and written communication
- Excellent presentation skills
- Excellent analytical, judgment, decision making and problem solving skills
- Excellent planning and organizing skills
- Excellent interpersonal skills to foster harmonious working environment
- Strong Customer Service and quality focus skills
- High level of integrity and confidentiality

### **Technical**

- Sound knowledge of applicable laws, policies, regulation and procedures
- Good knowledge of auditing techniques and practices
- Good knowledge of risk management techniques and strategies
- Knowledge of Corporate Governance Framework for Public Bodies in Jamaica.
- Good knowledge and understanding of GOJ policies and programmes and the machinery of government

- Understanding of data management and information security principles ,including encryption, access controls and risk management
- Good critical reasoning, quantitative and qualitative analysis skills
- Knowledge of change management principles and practices
- Strong environmental scanning, analysis and interpretive skills
- Strong negotiating and persuasive presentation skills
- Experience in conducting data protection impact assessments and developing privacy policies, procedures, and guidelines
- Experience with handling data breaches, incidents, and interactions with the Office of the Information Commissioner
- Proficiency in the use of the relevant computer applications

#### **MINIMUM REQUIRED EDUCATION AND EXPERIENCE:**

- Bachelors' degree in Computer Science, Audit or equivalent qualification from recognized tertiary institution
- Certification in Information Security, Data Protection and/or Privacy Certification such as CIPP, CIPT, ISEB, etc. (preferred)
- Exposure to legal training would be an asset
- Sound knowledge of the Data Protection Act and other applicable data protection policies.
- One (1) year related work experience

#### **AUTHORITY TO:**

- Recommend security procedures and maintenance for Data Protection
- Report breaches to the OIC
- Develop and review data protection policies
- Maintain risk and breach register
- Take remedial action for breaches
- Conduct training and sensitization relating to data protection
- Data Protection Security Audits

- Recommends appropriate standards
- Recommends improvements in corporate governance framework
- Recommends changes to regulatory framework
- Access to highly personal confidential and sensitive data/information

**SPECIFIC CONDITIONS ASSOCIATED WITH THE JOB:**

- Normal office working environment
- May be required to work beyond normal work hours in order to meet deadlines.
- May be required to work on public holidays/weekends
- Possession of a valid Drivers' Licence and a reliable motor vehicle.

**Salary Scale: \$3,501,526 - \$4,709,163**