ICO 25-93

Ministry of
Education & Youth

CAREER OPPORTUNITY

JOB TITLE : DATA PROTECTION OFFICER (GMG/SEG 2) - TEMPORARY

NATIONAL PARENTING SUPPORT COMMISSION
NATIONAL EDUCATION INSPECTORATE
JAMAICA TEACHING COUNCIL
JAMAICA TERTIARY EDUCATION COMMISSION
NATIONAL COLLEGE ON EDUCATIONAL LEADERSHIP

Under the general direction of the Chief Inspector, the Data Protection Officer is responsible for the ensuring the Ministry 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 the NEI and will ensure that sensitive data is protected in accordance with the law.

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

REMUNERATION PACKAGE:

Pay Band 8 Salary Scale: $4,266,270.00 to $5,737,658.00 p.a

Ministry of
Education & Youth

ICO 25-93

FOR FURTHER INFORMATION, PLEASE CONTACT THE DIRECTOR, HUMAN RESOURCE MANAGEMENT, AT EXT. 5883 INTERESTED PERSONS ARE INVITED TO SUBMIT APPLICATIONS WITH RÉSUMÉS NO LATER THAN WEDNESDAY, JUNE 25, 2025 TO THE ADDRESS PRESENTED BELOW.

DIRECTOR – HUMAN RESOURCE MANAGEMENT
MINISTRY OF EDUCATION & YOUTH
2 NATIONAL HEROES CIRCLE,
KINGSTON 4

WE THANK ALL APPLICANTS FOR EXPRESSING AN INTEREST; HOWEVER, ONLY SHORTLISTED CANDIDATES WILL BE CONTACTED.

CLICK HERE TO APPLY

EDUCATE Jamaica 2.0

MINISTRY OF EDUCATION & YOUTH
JAMAICA TEACHING COUNCIL
JOB DESCRIPTION AND SPECIFICATION

JOB TITLE:	Data Protection Officer
JOB GRADE:	Level 4
POST NUMBER:	**TMP15395SB**
AGENCY:	**Jamaica Teaching Council**
REPORTS TO:	Chief Executive Officer
MANAGES DIRECTLY:	N/A

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

_____
Manager/Supervisor Date

_____
Head of Department/Division Date

_____
Date received in Human Resource Division Date Created/revised

Job Purpose:

Under the general direction of the Chief Executive Officer, the Data Protection Officer is responsible for the ensuring the Ministry 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 the JTC 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 Jamaica Teaching Council (JTC) 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 the JTC 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 JTC 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 JTC;
- 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 JTC's privacy policies and procedures;
- Provides advice/information to the Ministry and its employees on their obligations under the Data Protection Act and state data protection provisions;
- Manages and conducts ongoing reviews of the JTC's Data Protection Framework;
- Disseminates current information on policies, procedures and legislation for the JTC'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 the JTC;
- 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 JTC's ICT Division 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 relevant officers from the Internal Audit Unit, Legal Services Unit and other key stakeholders to monitor, implement and analyse compliance programmes;
- Monitors to ensure that the JTC'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 Chief Executive Officer and the Executive Team of the JTC 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 Chief Executive Officer;

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

Contact (Title)	Purpose of Communication
Chief Executive Officer	To receive and provide guidance and technical advice
Internal Audit	To provide technical advice and guidance
ICT Division	To provide technical advice and guidance
Divisional/Branch/Unit Heads	To provide technical advice and guidance
Regional Offices	To provide technical advice and guidance
All Staff members	To provide technical advice and guidance

External

Contact (Title)	Purpose of Communication
Office of the Information Commissioner	To obtain and share information relating to the administration of the act
Ministries, Departments & Agencies	To receive and provide information, consultation
Regional/International Partners	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.

Validation of Job Description

This document is validated as an accurate and true description of the job described herein

_____	_____
Employee	Date
_____	_____
Manager/Supervisor	Date
_____	_____
Head of Department/Division	Date
_____	_____
Date received in Human Resource Division	Date Created/revised

MINISTRY OF EDUCATION & YOUTH
NATIONAL COLLEGE ON EDUCATIONAL LEADERSHIP
JOB DESCRIPTION AND SPECIFICATION

JOB TITLE:	Data Protection Officer
JOB GRADE:	GMG/SEG 2
POST NUMBER:	**TMP15072CG**
AGENCY:	National College of Educational Leadership
REPORTS TO:	Director/Principal
MANAGES DIRECTLY:	N/A

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

_____
Manager/Supervisor Date

_____
Head of Department/Division Date

_____
Date received in Human Resource Division Date Created/revised

Job Purpose:

Under the general direction of the Director/Principal; the Data Protection Officer is responsible for the ensuring the Ministry 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 NCEL 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 College Educational Leadership (NCEL) 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 the NCEL 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 NCEL 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 NCEL;
- 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 NCEL's privacy policies and procedures;
- Provides advice/information to the Board and its employees on their obligations under the Data Protection Act and state data protection provisions;
- Manages and conducts ongoing reviews of the NCEL's Data Protection Framework;
- Disseminates current information on policies, procedures and legislation for the Ministry'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 NCEL;
- 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 Ministry's ICT Division 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 relevant officers from the Internal Audit Unit, Legal Services Unit and other key stakeholders to monitor, implement and analyse compliance programmes;
- Monitors to ensure that the NCEL'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 Director/Principal and the Executive Team of the NCEL 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 Director/Principal,

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

Contact (Title)	Purpose of Communication
Director/Prinicpal	To receive and provide guidance and technical advice
Internal Audit	To provide technical advice and guidance
ICT Division	To provide technical advice and guidance
Divisional/Branch/Unit Heads	To provide technical advice and guidance
Regional Offices	To provide technical advice and guidance
All Staff members	To provide technical advice and guidance

External

Contact (Title)	Purpose of Communication
Office of the Information Commissioner	To obtain and share information relating to the administration of the act
Ministries, Departments & Agencies	To receive and provide information, consultation
Regional/International Partners	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.

Validation of Job Description

This document is validated as an accurate and true description of the job described herein

_____	_____
Employee	Date
_____	_____
Manager/Supervisor	Date
_____	_____
Head of Department/Division	Date
_____	_____
Date received in Human Resource Division	Date Created/revised

MINISTRY OF EDUCATION & YOUTH
NATIONAL EDUCATION INSPECTORATE
JOB DESCRIPTION AND SPECIFICATION

JOB TITLE:	Data Protection Officer
JOB GRADE:	GMG/SEG 2
POST NUMBER:	**TMP15073CG**
AGENCY:	National Education Inspectorate
REPORTS TO:	Chief Inspector
MANAGES DIRECTLY:	N/A

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

_____
Manager/Supervisor Date

_____
Head of Department/Division Date

_____
Date received in Human Resource Division Date Created/revised

Job Purpose:

Under the general direction of the Chief Inspector, the Data Protection Officer is responsible for the ensuring the Ministry 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 the NEI 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 Inspectorate (NEI) 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 the NEI 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 NEI 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 NEI;
- 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 NEI's privacy policies and procedures;
- Provides advice/information to the NEI and its employees on their obligations under the Data Protection Act and state data protection provisions;
- Manages and conducts ongoing reviews of the NEI's Data Protection Framework;
- Disseminates current information on policies, procedures and legislation for the NEI'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 the NEI;
- 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 MoEY's ICT Division 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 relevant officers from the Internal Audit Unit, Legal Services Unit and other key stakeholders to monitor, implement and analyse compliance programmes;
- Monitors to ensure that the NEI'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 Chief Inspector and the Executive Team of the NEI 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 Chief Inspector,

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

Contact (Title)	Purpose of Communication
Chief Inspector	To receive and provide guidance and technical advice
Internal Audit	To provide technical advice and guidance
ICT Division	To provide technical advice and guidance
Divisional/Branch/Unit Heads	To provide technical advice and guidance
Regional Offices	To provide technical advice and guidance
All Staff members	To provide technical advice and guidance

External

Contact (Title)	Purpose of Communication
Office of the Information Commissioner	To obtain and share information relating to the administration of the act
Ministries, Departments & Agencies	To receive and provide information, consultation
Regional/International Partners	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.

Validation of Job Description

This document is validated as an accurate and true description of the job described herein

_____	_____
Employee	Date
_____	_____
Manager/Supervisor	Date
_____	_____
Head of Department/Division	Date
_____	_____
Date received in Human Resource Division	Date Created/revised

MINISTRY OF EDUCATION & YOUTH
NATIONAL PARENTING SUPPORT COMMISSION
JOB DESCRIPTION AND SPECIFICATION

JOB TITLE:	Data Protection Officer
JOB GRADE:	
POST NUMBER:	**TMP15396SB**
AGENCY:	**National Parenting Support Commission**
REPORTS TO:	Chief Executive Officer
MANAGES DIRECTLY:	N/A

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

_____
Manager/Supervisor Date

_____
Head of Department/Division Date

_____
Date received in Human Resource Division Date Created/revised

Job Purpose:

Under the general direction of the Chief Executive Officer, the Data Protection Officer is responsible for the ensuring the Ministry 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 the NPSC 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 Parenting Support Commission (NPSC) 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 the NPSC 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 NPSC 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 NPSC;
- 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 NPSC's privacy policies and procedures;
- Provides advice/information to the NPSC and its employees on their obligations under the Data Protection Act and state data protection provisions;
- Manages and conducts ongoing reviews of the NPSC's Data Protection Framework;
- Disseminates current information on policies, procedures and legislation for the Ministry'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 the NPSC;
- 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 Ministry's ICT Division 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 relevant officers from the Internal Audit Unit, Legal Services Unit and other key stakeholders to monitor, implement and analyse compliance programmes;
- Monitors to ensure that the NPSC'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 Chief Executive Director and the Management Team of the NPSC 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 Chief Executive Officer,

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

Contact (Title)	Purpose of Communication
Chief Executive Officer	To receive and provide guidance and technical advice
Internal Audit	To provide technical advice and guidance
ICT Division	To provide technical advice and guidance
Divisional/Branch/Unit Heads	To provide technical advice and guidance
Regional Offices	To provide technical advice and guidance
All Staff members	To provide technical advice and guidance

External

Contact (Title)	Purpose of Communication
Office of the Information Commissioner	To obtain and share information relating to the administration of the act
Ministries, Departments & Agencies	To receive and provide information, consultation
Regional/International Partners	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.

Validation of Job Description

This document is validated as an accurate and true description of the job described herein

_____	_____
Employee	Date
_____	_____
Manager/Supervisor	Date
_____	_____
Head of Department/Division	Date
_____	_____
Date received in Human Resource Division	Date Created/revised

JAMAICA TERTIARY EDUCATION COMMISSION
JOB DESCRIPTION AND SPECIFICATION

JOB TITLE:	Data Protection Officer
JOB GRADE:	GMG/SEG 2
POST NUMBER:	**TMP15071CG**
AGENCY:	Jamaica Tertiary Education Commission
REPORTS TO:	Commissioner/Chief Executive Officer
MANAGES DIRECTLY:	N/A

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

_____
Manager/Supervisor Date

_____
Head of Department/Division Date

_____
Date received in Human Resource Division Date Created/revised

Job Purpose:

Under the general direction of the Commissioner/Executive Director, the Data Protection Officer is responsible for the ensuring the Ministry 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 the JTEC 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 Jamaica Tertiary Education Commission (JTEC) 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 the JTEC 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 JTEC 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 JTEC;
- 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 JTEC's privacy policies and procedures;
- Provides advice/information to the JTEC and its employees on their obligations under the Data Protection Act and state data protection provisions;
- Manages and conducts ongoing reviews of the JTEC's Data Protection Framework;
- Disseminates current information on policies, procedures and legislation for the JTEC'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 the JTEC;
- 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 JTEC's ICT Division 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 relevant officers from the Internal Audit Unit, Legal Services Unit and other key stakeholders to monitor, implement and analyse compliance programmes;
- Monitors to ensure that the JTEC'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 Commissioner/Chief Executive Officer and the Executive Team of the JTEC 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 Commissioner/Chief Executive Officer,

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

Contact (Title)	Purpose of Communication
Commissioner/Chief Executive Officer	To receive and provide guidance and technical advice
Internal Audit	To provide technical advice and guidance
ICT Division	To provide technical advice and guidance
Divisional/Branch/Unit Heads	To provide technical advice and guidance
Regional Offices	To provide technical advice and guidance
All Staff members	To provide technical advice and guidance

External

Contact (Title)	Purpose of Communication
Office of the Information Commissioner	To obtain and share information relating to the administration of the act
Ministries, Departments & Agencies	To receive and provide information, consultation
Regional/International Partners	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.

Validation of Job Description

This document is validated as an accurate and true description of the job described herein

_____	_____
Employee	Date
_____	_____
Manager/Supervisor	Date
_____	_____
Head of Department/Division	Date
_____	_____
Date received in Human Resource Division	Date Created/revised