

Ministry of Education

Cayman Islands Government

Version 1.0

Data Protection Policy

Table of Contents

1. EXECUTIVE SUMMARY 1

2. INTRODUCTION 1

2.1 Background 1

2.2 Purpose and Objectives 1

2.3 Scope 2

3. LEGISLATIVE FRAMEWORK 2

4. DEFINITIONS AND ABBREVIATIONS 3

5. ROLES AND RESPONSIBILITIES 6

6. POLICY REQUIREMENTS 7

6.1 Data Inventory, Data Mapping and Record of Processing Activities (RoPA) 7

6.2 Data Protection Impact Assessments 7

6.3 Data Protection Principles 8

6.4 Purpose Limitation and Data Minimisation 9

6.5 Legal Bases/Conditions of Processing 9

6.6 Consent 10

6.7 Privacy Notices 11

6.8 Individual Rights 12

6.9 Data Subject Access Requests (DSARs) 15

6.10 Data Accuracy 16

6.11 Security 17

6.12 Sharing Data with Joint Data Controllers, Data Processors and Third Parties 18

6.13 International Transfers 19

6.14 Incident Reporting and Response 20

6.15 Personal Data Breach Notification 21

6.16 Data Retention and Disposal 22

6.17 Acting as a Data Processor 23

6.18 Exemptions 23

6.19 Training and Awareness 23

7. DATA PROTECTION LEADER 23

8 POLICY EVALUATION AND CHANGE 24

1. EXECUTIVE SUMMARY

This Data Protection Policy ("this Policy") establishes how the Ministry of Education ("the Ministry") protects Personal Data based on the Cayman Islands Data Protection Act (2021 Revision) ("DPA") and Data Protection Regulations, 2018 ("Regulations") and in line with the **Cayman Islands Government ("CIG") Privacy Policy**.

This Policy ensures the Ministry's employees and other Public Officials and suppliers who have access to personal data processed by the Ministry understand the rules governing the use of Personal Data.

2. INTRODUCTION

2.1 Background

When delivering public policies, programmes and services, the Ministry may collect, store and use Personal Data, including but not limited to Personal Data relating to individuals residing in the Cayman Islands, visitors to the Cayman Islands, Civil Servants, other Public Officials, affiliates, and suppliers and service providers. In most cases, the Personal Data processed by the Ministry will be provided directly by the individual (i.e. the Data Subject). However, the Ministry may also receive Personal Data indirectly (e.g. when conducting a background check or from another Public Authority in the course of their duties).

Against this background, the Ministry:

i. Must only use Personal Data to deliver public policies, programmes and services, including under enabling legislation, and for other legitimate purposes.

ii. Is responsible for the protection of Personal Data under its control and compliance with applicable privacy laws, including the DPA and Regulations, and the CIG Privacy Framework.

iii. Will, where necessary, consult and comply with the provisions of the European Union's General Data Protection Regulation where such consultation or compliance becomes necessary, and subject to legal advice from the Solicitor General.

2.2 Purpose and Objectives

Implementing and complying with this Policy will enable the Ministry's success by maintaining the public's trust in the handling of Personal Data to make the lives of those we serve better. It aims to minimise risk of breach of privacy laws and any resulting complaints and/or enforcement action, including monetary penalties.

The objectives of this Policy are to:

i. Facilitate the Ministry's statutory and regulatory compliance in accordance with legislative framework;
ii. Promote consistency in practices and procedures in administering the CIG Privacy Policy; and
iii. Ensure effective protection and management of Personal Data throughout its collection, use, disclosure, retention and disposal.

2.3 Scope

This Policy applies to all employees of the Ministry of Education, all Data Processors engaged by the Ministry, and all other Public Officials, suppliers and service providers that process Personal Data on behalf of or that have access to Personal Data where the Ministry is the Data Controller, a Joint Data Controller, or a Data Processor. This Policy must be read in combination with all legislation relevant to the Ministry; all relevant CIG policies and procedures; and all policies, procedures and other documentation specifically relevant to data protection in the Ministry, including Privacy Notices, Memoranda of Understanding (MOUs), Data Processing Agreements and Terms of Service.

This Policy covers the operations of all Departments, sections and units within the Ministry of Education, including the Department of Education Services and the Cayman Islands Public Library Services. It also covers the operations of the Education Council, the CXC National Committee and the Public Libraries Management Committee. Throughout this Policy, "the Ministry" must be read as including all departments and statutory bodies within the ministerial portfolio of responsibilities where the policy statement relates to the duties of a Data Controller as defined under the DPA.

This Policy does not cover the operations of the University College of the Cayman Islands.

3. LEGISLATIVE FRAMEWORK

The following provisions shall be read and construed in conjunction with this Policy:

i. Cayman Islands Constitution Order
ii. Confidential Information Disclosure Act, 2016
iii. Data Protection Act (2021 revision) and the Data Protection Regulations, 2018
iv. Education Law, 2016
v. Education Regulations, 2017
vi. Electronic Transactions Act (2011 Revision)
vii. Evidence Act (2011 Revision)
viii. Freedom of Information Act (2021 Revision) and the Freedom of Information Regulations (2021 Revision)
ix. Information and Communications Technology Act (2017 Revision)
x. National Archive and Public Records Act (2015 Revision) and the National Archive and Public Records Regulations, (2007)
xi. Procurement Act, 2016 and the Procurement Regulations (2022 Revision)
xii. Public Service Management Act (2018 Revision) and Personnel Regulations (2022 Revision)

The DPA along with the Regulations serve as the key enabling legislation for this Policy. As a Public Authority, The Ministry of Education is also subject to the National Archive and Public Records Act (2015 Revision) read with the National Archive and Public Records Regulations, 2007; the Public Service Management Act (2018 Revision) read with the Personnel Regulations (2022 Revision); and other legislation.

This Policy shall also be read together with the following:

i. Cayman Islands Government Information Security Policy;
ii. Cayman Islands Government- Security Incident Procedure; and

iii. Information Security in Procurement Supply Chain.
iv. Records Management Policy
v. Risk Management Framework
vi. Social Media Policy
vii. Record Management Standard S1: Creation, Maintenance and Disposal
viii. Record Management Standard S2: Records and Information Management Standard
ix. Whistle Blower Policy

4. DEFINITIONS AND ABBREVIATIONS

Cayman Islands Data Protection Act (2021 Revision) ("DPA"): Legislation enacted by the Parliament of the Cayman Islands that applies to the Processing of Personal Data, including by all Public Authorities.

Cayman Islands Freedom of Information Act (2021 Revision) ("FOIA"): Legislation enacted by the Parliament of the Cayman Islands that grants the public a general right of access to records held by Public Authorities.

Cayman Islands Government ("CIG"): The Cayman Islands Government. See section 2.3 for the scope of this Policy.

Child: An individual under the age of 18 years.

Civil Servant: In accordance with the Public Service Management Act (2018 Revision), "means a person employed by the government, but does not include a Member of the Legislative Assembly other than an Official Member."

Consent: In accordance with the DPA, "any freely given, specific, informed and unambiguous indication of the data subject's wishes by which the data subject, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to the said data subject." Refer to Schedule 5 of the DPA for additional conditions of Consent.

Data Controller: In accordance with the DPA, "the person who, alone or jointly with others determines the purposes, conditions and manner in which any personal data are, or are to be, processed." For the purposes of this Policy, and with attention to the definition of Person in the DPA (reproduced in this section), this Ministry is considered to be a Data Controller.

Data Processing Agreement: A Data Processing Agreement is a legally binding contract that states the rights and obligations of each party (i.e. Data Controller and Data Processor) concerning the protection and Processing of Personal Data.

Data Processor: In accordance with the DPA, "any person who processes personal data on behalf of a data controller but, for the avoidance of doubt, does not include an employee of the data controller." For the avoidance of doubt, Person has the meaning assigned in the DPA (reproduced in this section) and one Public Authority may serve as a Data Processor for a separate Public Authority that is the Data Controller. A Public Authority may also engage a non-CIG Data Processor.

Data Protection Impact Assessment ("DPIA"): A DPIA is a process designed to help in systematically analysing, identifying and minimising the data protection risks of a project or plan.

Data Protection Principles: In accordance with the DPA, eight core Data Protection Principles referred to in section 5 of the DPA and listed in Schedule 1 of the DPA.

Data Subject: In accordance with the DPA, "an identified living individual; or a living individual who can be identified directly or indirectly by means reasonably likely to be used by the data controller or by any other person."

Data Subject Rights: Rights individuals have in relation to their own Personal Data under the DPA. These rights are not absolute, as all but one may be restricted or subject to modifications in certain specified circumstances. Exemptions from these rights may also apply, whereby specified rights or other provisions of the DPA do not apply.

DPA Data Protection Regulations, 2018: Regulations made under the DPA.

European Union General Data Protection Regulation ("GDPR"): Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data. [Note: The GDPR does not apply to the CIG as a whole but may apply to certain activities undertaken by Public Authorities, based on the nature of their operations. See Article 3 of the GDPR (Territorial scope) for more information.]

Inaccurate Personal Data: Personal Data that are inaccurate, including because they are misleading, incomplete or out of date.

Information Rights Unit: The section of the Cabinet Office tasked with leading and coordinating data protection across government and developing internal capacity for compliance.

Joint Data Controllers: When two or more Data Controllers jointly determine the purposes and means of Processing.

Memorandum of Understanding ("MOU"): A formal, written record of understanding between two or more parties that outlines the terms and conditions that will govern the sharing of Personal Data between the parties or that will govern the disclosure of Personal Data from one party to another party that is considered a Third Party.

Office of the Ombudsman of the Cayman Islands ("Ombudsman"): The supervisory authority for data protection related matters, who investigates, mediates and decides on complaints about the rights of Data Subjects and how the Personal Data of Data Subjects is being used.

Person: In accordance with the DPA, "any corporation, either aggregate or sole, and any club, society, association, public authority or other body, of one or more persons."

Personal Data: In accordance with the DPA, "data relating to a living individual who can be identified and includes data such as the living individual's location data, online identifier or one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of the living individual; an expression of opinion about the living individual; or any indication of the intentions of the data controller or any other person in respect of the living individual."

Personal Data Breach: In accordance with the DPA, "a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of or, access to, personal data transmitted, stored or otherwise processed."

Privacy Framework: A set of high-level CIG policies and related detailed procedures that form the basis for enabling data protection practices that support privacy by design concepts, help the CIG protect Data Subjects' privacy, and demonstrate excellence in governance practices. The CIG Privacy Framework is complemented by various levels of documentation, which may be developed by a specific Public Authority.

Privacy Notice: A statement used to communicate information to Data Subjects about why and how their Personal Data will be processed, including steps taken by the Data Controller to comply with the DPA.

Processing [/Process/Processed]: In accordance with the DPA, "obtaining, recording or holding data, or carrying out any operation or set of operations on personal data, including organising, adapting or altering the personal data; retrieving, consulting or using the personal data; disclosing the personal data by transmission, dissemination or otherwise making it available; or aligning, combining, blocking, erasing or destroying the personal data."

Process Owner: The individual who is accountable for the performance of a process that includes processing of personal data and who manages that process on a daily basis.

Public Authority: In accordance with the DPA, "a ministry, portfolio or department; a statutory body or authority, whether incorporated or not; a company which is wholly owned by the Government or in which the Government has a direct or indirect controlling interest; or is specified in an Order made by the Cabinet; and any other body or organisation specified by the Cabinet by Order as a public authority on account of providing services of a public nature which are essential to the welfare of Caymanian society."

Public Official: In accordance with the Cayman Islands Constitution Order 2009, "includes any organisation or person carrying out a public function or duty, including the Governor, except where the nature of their act is private".

Recipient: In accordance with the DPA, "a person to whom the data are disclosed, as well as any person (such as an employee or agent of the relevant data controller, a relevant data processor, or an employee or agent of a data processor) to whom they are disclosed in the course of processing the data for the data controller, but does not include a person to whom disclosure is or may be made as a result of, or with a view to, a particular inquiry by or on behalf of that person made in the exercise of any power conferred by law."

Risk Owner: In accordance with the Cayman Islands Government Risk Management Framework, "the individual who is responsible for ensuring the risk is mitigated appropriately."

Record of Processing Activities ("RoPA"): A Record of Processing Activities is written documentation and overview of procedures by which Personal Data are processed. RoPAs must include information about data Processing, including types of Personal Data that are processed, categories of Data Subjects, the purpose of the Processing and any Recipients.

Sensitive Personal Data: In accordance with the DPA, "personal data consisting of the racial or ethnic origin of the data subject; the political opinions of the data subject; the data subject's religious beliefs or other beliefs of a similar nature; whether the data

subject is a member of a trade union; genetic data of the data subject; the data subject's physical or mental health or condition; medical data; the data subject's sex life; the data subject's commission, or alleged commission, of an offence; or any proceedings for any offence committed, or alleged, to have been committed by the data subject, the disposal of any such proceedings or any sentence of a court in the Islands or elsewhere."

Third Party: In accordance with the DPA, "in relation to personal data, means any person other than the data subject; the data controller; or any data processor or other person authorised to process data for the data controller or data processor."

5. ROLES AND RESPONSIBILITIES

Data protection roles and responsibilities across the CIG are outlined in section 6 of the **CIG Privacy Policy**. Whilst every Ministry personnel has a role to play, as outlined in this Policy, the following table summarizes the fundamental data protection roles and responsibilities within the Ministry:

Functions	**Chief Officer**	**Data Protection Leader**
Documenting Operating Procedures	**A**	**R**
Data Protection Audit Controls	**A**	**R**
Data Processing Agreements	**A**	**R**
MOUs for Data Controller to Data Processor Relationships	**A**	**R**
Monitoring and review of supplier relationships	**A**	**R**
Managing Changes to suppliers	**A**	**R**
Responsibilities for Data Protection Incident Management	**A**	**R**
Events reported internally	**A**	**S**
Assessment of and decision on Personal Data Breach event	**A/R**	**S**
Reporting Personal Data Breaches to Ombudsman	**A**	**R**
Responding to personal data breaches	**A**	**R**
Post-event assessment	**A**	**R**
Collection of evidence	**A**	**S**
Planning of Data Subjects Rights	**A**	**R**
Implementing and managing the process for Data Subject Rights (excluding DSARs)	**A**	**R**
Maintaining data subjects' records	**A**	**S**
Processing Data Subject Access Requests (DSARs)	**A**	**S**
Identifying applicable legislation and contractual requirements	**A**	**R**
Compliance with relevant policies and standards	**A**	**S**
Independent review of Data Protection	**A**	**S**
Contact with the Ombudsman	**A**	**R**

Key: A-Accountable, R-Responsible, S-Supporting

6. POLICY REQUIREMENTS

6.1 Data Inventory, Data Mapping and Record of Processing Activities (RoPA)

6.1.1 The Ministry will aim to comprehensively inventory and map the processing of Personal Data undertaken and keep these records up-to-date.

6.1.2 The Ministry will work towards creating and maintaining a RoPA and keep an overview of all processing activities undertaken.

6.1.3 The Ministry shall ensure any RoPA includes the following as a Data Controller or a Joint Data Controller:

i. The Ministry's name and contact details, (and, where applicable, the name of the Joint Data Controller, their representative and the Data Protection Leader);
ii. the purposes for the processing of Personal Data;
iii. a description of the categories of Data Subjects and categories of Personal Data;
iv. the categories of Recipients of Personal Data;
v. details of transfers to any countries or territories outside of the Cayman Islands, including a record of the transfer mechanism and safeguards in place;
vi. retention schedules, which may reference the relevant disposal schedule; and
vii. a description of the technical and organisational security measures in place.

6.1.4 The Ministry will create and maintain an internal record of all processing activities carried out by Data Processors on behalf of the Ministry, which shall be at a high level and note the types of processing activities that may be carried out generally. This requirement may be met through the maintenance of sufficiently detailed Data Processing Agreements, MOUs and Terms of Service.

6.1.5 The Ministry will keep under review and update data inventories, data maps and the RoPA at appropriate intervals, at least annually, and as soon as practicable when there are changes to services and programmes, purposes for processing Personal Data, new Recipients of Personal Data, new technologies, and/or legislative changes.

6.2 Data Protection Impact Assessments (DPIAs)

6.2.1 The Ministry shall, when introducing new processes, services, programmes or technologies that process Personal Data, or in the event of a significant change to an existing process, service, programme or technology that processes Personal Data, assess whether this processing poses a high risk to the privacy and other rights and freedoms of Data Subjects.

6.2.1 In determining whether processing of Personal Data poses a high risk to the rights and freedoms of Data Subjects, the Ministry shall consider the nature, scope, context and purpose of the processing.

6.2.2 As part of the risk analysis, the Ministry may carry out an assessment of the impact of the planned processing on the protection of Personal Data using established DPIA procedures.

6.2.3 The process owners (the employee who is accountable for the performance of the process that includes processing of personal data and who manages that process on a daily basis) is responsible for completing Data Protection Impact Assessments.

6.2.4 The Data Protection Leader must be consulted to support this activity by providing advice on appropriate measures to manage risk and ultimately, recommending whether the processing activity may proceed as planned.

6.2.5 Where the Ministry is drawing up administrative measures or rules relating to the protection of Data Subjects' rights and freedoms with regard to Personal Data processing, the Ministry shall, as required by the DPA, consult the Ombudsman on the content of such measures or rules in accordance with the guidelines issued by the Ombudsman and using the relevant consultation form.[1]

6.2.6 The Ministry's Template DPIA is appended to this Policy for reference purposes.

6.3 Data Protection Principles

6.3.1 The Ministry is a Data Controller, having determined the purposes, conditions and manner in which Personal Data are processed, and is responsible for complying with the DPA, including the Data Protection Principles, in relation to these processing activities.

6.3.2 The Department of Education Services, Cayman Islands Public Library Service, Education Council, CXC National Committee and other statutory bodies within the Ministry's portfolio of responsibilities will also be Data Controllers where they determine the purposes, conditions and manner in which Personal Data are processed. Where these departments or statutory bodies are the Data Controller, they are responsible for complying with the DPA, including the Data Protection Principles, in relation to these processing activities.

6.3.3 The Data Protection Principles define the Data Controller's responsibilities in protecting Personal Data. All employees and all other Public Officials (including members of boards and committees) and suppliers that have access to or Process Personal Data on behalf of the Ministry must handle Personal Data in alignment with these principles.

6.3.4 To ensure the obligations under the DPA are met, the processing of Personal Data must comply with the principles of the DPA, unless limited exceptions and exemptions apply. Accordingly, Personal Data will be:

i. Processed lawfully, fairly and in a transparent manner in relation to the Data Subject;
ii. Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;
iii. Adequate, relevant, and limited to what is necessary in relation to the purposes for which they are collected or further Processed;
iv. Accurate and, where necessary, kept up-to-date; every reasonable step must be taken to ensure that Inaccurate Personal Data, having regard to the purpose for which they are Processed, are rectified, blocked, erased or destroyed without delay;
v. Kept for only as long as it is needed and subsequently destroyed; the Ministry will ensure the purposes of Processing clearly include the legal obligation as a public agency to maintain public records in accordance with the National Archive and Public Records Act (2015 Revision) and to only destroy public records in accordance with an approved disposal schedule;
vi. Processed in accordance with the rights of Data Subjects, including under the DPA;

[1] Note: These guidelines and this form can be downloaded from ombudsman.ky, in the "Resources" section of the website.

vii. Processed in a manner that ensures appropriate security of the Personal Data, including protection against unauthorised or unlawful Processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures; and
viii. Transferred only to countries or territories which ensure there is an adequate level of protection for the rights and freedoms of Data Subjects in relation to the Processing of Personal Data.

6.4 Purpose Limitation and Data Minimisation

This section describes how the principles of purpose limitation and data minimisation will be met by the Ministry. It is a minimum requirement of the DPA to comply with these Data Protection Principles. In order to comply with the requirement to provide Privacy Notices, all purpose for processing must be documented.

6.4.1 The Ministry shall clearly identify and document the purposes for processing Personal Data. These purposes shall be contained in the Data Mapping and Inventory Document and/or the initial Data Protection Impact Assessment document.
6.4.2 The Ministry will ensure that the purposes for processing Personal Data are included in its Privacy Notices. See **Privacy Notices** (section 6.7) for more details.
6.4.3 The Ministry shall ensure that when new purposes for processing Personal Data are identified, it is satisfied that one of the following applies:
i. The new purpose is not incompatible with the original purpose; or
ii. The processing is exempt from the second Data Protection Principle (purpose limitation) pursuant to a specific provision in Part 4 of the DPA
iii. The Ministry has identified the legal basis or legal bases requiring or allowing the new processing – for example, a new legal obligation or function – and is able to ensure the processing will be fair and in compliance with the DPA.
6.4.4 The Ministry will ensure that all Personal Data collected at all times or further processed is adequate, relevant and limited to what is necessary in relation to the purposes for which the Personal Data are being processed or will be processed.
6.4.5 The Ministry will ensure that when Personal Data are no longer needed for specified purposes, they are destroyed, secured, archived or anonymised in accordance with the data retention guidelines. See **Data Retention and Disposal** (section 6.16) for more details.
6.4.6 The Ministry will ensure that only the minimum amount of Personal Data needed to fulfil the purpose or purposes are requested, collected, accessed, shared, disclosed or otherwise Processed.
6.4.7 The Ministry will review its data processing periodically to check that the Personal Data held are still relevant and adequate for the purposes of processing.

6.5 Legal Bases/Conditions of Processing

This section describes the legal bases for processing Personal Data, known as “conditions” of processing in the DPA, and how the Ministry will ensure processing is lawful by meeting at least one of these legal bases for each purpose of processing.

6.5.1 It is the Ministry’s responsibility to understand the different legal bases for processing Personal Data and ensure that there is a legal basis for processing Personal Data and an additional legal basis for processing Sensitive Personal Data. Some legal bases have different requirements depending on the purpose of collection. The requirement to have

a legal basis or legal bases for processing applies to the disclosure of Personal Data as well as to providing access to Personal Data between the Ministry and other Data Controllers, including other Public Authorities that may or may not be within the Ministry's portfolio of responsibilities.

6.5.2 The Ministry shall ensure that one or more legal bases will be satisfied whenever Personal Data are processed and will work towards identifying and documenting the legal basis or legal bases relied upon in relation to the processing of Personal Data and Sensitive Personal Data for each specific purpose or group of related purposes. The Legal bases will be documented in the DPIA document for each processing activity undertaken by the Ministry.

6.5.3 The Ministry shall ensure that the legal basis or legal bases for processing of Personal Data and Sensitive Personal Data are identified in advance and that all processing of Personal Data and Sensitive Personal Data complies with the DPA.

6.5.4 The Ministry shall document and review the legal bases of its Personal Data and Sensitive Personal Data processing activities, including any information that may be recorded in RoPAs, this Policy, Privacy Notices, MOUs and other documentation (if applicable), at appropriate intervals to ensure compliance with the DPA and promote accountability.

6.5.5 For the avoidance of doubt, the Legal Bases for processing Personal and Sensitive Personal Data[2] are as follows:

PERSONAL DATA	**SENSITIVE PERSONAL DATA**
Consent	Consent
Contract	Employment
Legal Obligation	Vital Interests
Vital Interests	Non-Profit Associations
Public Functions	Information Made Public by the Data Subject
Legitimate Interests	Legal Proceedings
	Public Functions
	Medical Purposes
	Prescribed by Regulations

6.6 Consent

For the Ministry, processing necessary to comply with legal obligations or for the exercise of public functions is core to its legal basis for processing. There is no hierarchy between the legal bases for processing of Personal Data, of which a Data Subject's Consent is one option. Where there is a significant imbalance between the position of the Data Subject and Ministry, Consent shall not provide a legal basis for the processing. Where Consent is relied upon as a legal basis for processing, it must be valid and Schedule 5 of the DPA applies. Therefore, the following must be adhered to:

6.6.1 To ensure the validity of any consent obtained:

i. The Data Subject must give Consent prior to the processing;

ii. The request for Consent must be in an intelligible and easily accessible form, using plain and clear language, and require the Data Subject to make a

[2] See Schedules 2 and 3 of the DPA for a full outline of the conditions. The Ombudsman's Guide for Data Controllers also covers these matters in more detail.

statement or to take a clear affirmative action that is separate from any declaration that may be made at the same time concerning another matter;

iii. The Consent must be freely given, specific, informed and unambiguous;

iv. What the Data Subject has given Consent to (i.e. the purpose(s)) must be clearly documented;

v. When and how the Data Subject has given Consent must be able to be proven;

vi. The Data Subject must be able to withdraw the Consent at any time; and

vii. The processing of Personal Data on the basis of Consent must be stopped if Consent is withdrawn.

6.6.2 The declaration of Consent should be obtained in writing or electronically for the purposes of documentation. In some circumstances, and provided no other law requires written Consent for the processing, Consent may be given verbally or through a clear, affirmative action. The granting of Consent should always be documented in a way that will allow the Ministry to prove the Consent was given.

6.6.3 Where any Consent for children is required, the Ministry will ensure verifiable Consent of the Data Subject's parent(s)/guardian(s) is obtained or age-verification and/or competence-verification measures are implemented as necessary.

6.6.4 The Ministry will review and refresh Consent at regular intervals if necessary.

6.7 Privacy Notices

Under the DPA the Ministry is required to provide information to Data Subjects on the purposes for which their Personal Data are processed. The Ministry may also be required to provide additional detailed, specific information about its processing activities, including in response to a Data Subject Access Request (DSAR). The Ministry will ensure that appropriate Privacy Notices are in place advising Data Subjects how and why their Personal Data are being processed and advising them of their rights. The Ministry's External Privacy Notice is appended to this Policy.

6.7.1 Information about Personal Data processing must be provided through appropriate Privacy Notices, which must be concise, transparent, intelligible, easily accessible and communicated in clear and plain language.

6.7.2 Privacy Notices must contain, at minimum, the Ministry's identity and the purpose(s) for processing the Personal Data. The purpose(s) must be described in sufficient detail as to be meaningful and understandable to the Data Subject and not overly general in nature.

6.7.3 Privacy Notices (e.g. a Cookie Notice, External Privacy Notice and Employee Privacy Notice) for the Ministry will be developed, implemented and reviewed on an annual basis or upon changes to the purposes, legislative framework, processes, procedures and/or technologies.

6.7.4 The Ministry will update its Privacy Notices and communicate the changes to Data Subjects before starting any new processing if Personal Data will be used for a new purpose that is incompatible with the original purpose.

6.7.5 Privacy Notices may also explain, among other items, the legal basis/bases for processing the Personal Data, categories of Personal Data collected, how the Personal Data will be used, Data Subject Rights, potential Recipients of the Personal Data, applicable retention periods and security measures.

6.7.6 Privacy Notices should be adapted for either written or verbal communication of key information and generally provided directly to the Data Subject at the time the Personal

Data are collected, e.g. as part of an application form, an intake interview, or any other similar process.

6.7.7 Privacy Notices for Data Subjects that are not employees of the Ministry, including Cookie Notices, shall be published on the Ministry's website and shall be publicly accessible and easily identified by Data Subjects.

6.7.8 The Employee Privacy Notice shall be published or otherwise made readily available internally and shall be easily identified and accessible by all employees of the Ministry.

6.8 Individual Rights

The Ministry will process Personal Data in accordance with Data Subjects' rights. This means that ensuring that there are measures implemented that allow individuals to exercise their rights under relevant legislation, including the DPA. Furthermore, the Ministry will respect and honour these rights in compliance with the legislative framework.

In accordance with the DPA, Data Subjects have rights in relation to their own Personal Data, which include:

6.8.1 **The right to be informed**: The right of Data Subjects to obtain information regarding why and how their Personal Data are processed by the Ministry, with limited exemptions. In this regard, the Data Subject shall receive information directly or be referred to the Privacy Notice published by the Ministry provided that the Privacy Notice provides all of the required information.

6.8.2 **The right of access**: The right to request access to the Personal Data maintained by the Ministry on the Data Subject and to supplementary information about the processing, with limited exemptions.

i. All Ministry employees are required to be trained on how to recognise a DSAR and understand when a DSAR applies.

ii. All Ministry employees are required to immediately report a DSAR to the Data Protection Leader. See **Data Subject Access Requests (DSARs)** (section 6.9) for more details.

6.8.3 **Rights in relation to inaccurate data**: The right for Inaccurate Personal Data processed by the Ministry to be rectified, blocked, erased or destroyed. The Data Protection Principles require Personal Data to be accurate and, where necessary, kept up to date. An order from the Ombudsman following a complaint may also require the Ministry to rectify, block, erase or destroy inaccurate Personal Data.

i. All Ministry employees are required to be trained on how to recognise a complaint in relation to Inaccurate Personal Data and the policies and procedures in place to address Inaccurate Personal Data in the absence of an order from the Ombudsman.

ii. All Ministry employees are required to immediately report complaints regarding Inaccurate Personal Data to the Data Protection Leader.

iii. The Ministry shall ensure there are processes in place to respond without undue delay to a complaint or request from a Data Subject in relation to Inaccurate Personal Data.

iv. The Ministry will ensure that Data Subjects are informed, if and when the Ministry rectifies, blocks, erases or destroys any inaccurate Personal Data following a complaint or request from the Data Subject or an order from the Ombudsman.

v. Where a complaint in relation to inaccurate Personal Data will not lead to further action or a request from the Data Subject to rectify, block, erase or destroy Personal Data is lawfully denied, the Ministry will respond to the Data Subject in a timely manner and explain the reasons for closing the complaint or denying the request.
vi. All complaints received by the Ministry's employees in relation to inaccurate Personal Data and requests to rectify, block, erase or destroy Personal Data, must be reported to the Data Protection Leader who will maintain an up-to-date log of complaints.
vii. The Ministry's Data Protection Leader will maintain an up-to-date log of orders from the Ombudsman to rectify, block, erase or destroy inaccurate Personal Data and action taken by the Ministry to comply with such orders.
viii. The Ministry will ensure that appropriate systems are in place to rectify inaccurate Personal Data or ensure same can be blocked, erased or destroyed if rectification is not possible or appropriate in the circumstances. See **Data Accuracy** (section 6.10) for more details.

6.8.4 **The right to restrict or stop processing**: The right to stop or restrict the Ministry's use of Personal Data relating to the Data Subject, under certain conditions.
i. All Ministry employees are required to be trained on how to recognise a notice from a Data Subject to stop or restrict processing of Personal Data.
ii. All Ministry employees are required to immediately report notices to stop or restrict processing of Personal Data to the Data Protection Leader. The Data Protection Leader will maintain an up-to-date log of such notices.
iii. The Ministry will respond without undue delay to a notice from a Data Subject's request to stop or restrict processing of their Personal Data in whole, in relation to certain purposes, in certain manners.
iv. The Ministry will inform Data Subjects if and when the processing of their Personal Data has been stopped or restricted in accordance with a notice from the Data Subject.
v. If a notice to stop or restrict processing of Personal Data is lawfully denied, the Ministry will respond to the Data Subject with the reason why it will not comply with the notice. This response will be provided to the Data Subject as soon as practicable and, in any event, within 21 calendar days of receiving the notice in writing.
vi. The Ministry will identify and document situations where a Data Subject has applied to the Ombudsman following the Ministry's failure to comply with a notice or request to stop or restrict processing their Personal Data.
vii. The Ministry will ensure there are processes in place to stop or restrict processing of Personal Data on its systems without undue delay.
viii. Where applicable, the Ministry will ensure there are processes in place to indicate that processing of Personal Data is restricted on its systems.

6.8.5 **The right to stop direct marketing:** The right that a Data Subject has to cease the use of their Personal Data for direct marketing purposes by the Ministry.

At this time, the Ministry does not conduct any direct marketing as defined under the DPA and recognises that if it chooses to conduct direct marketing in the future, it must comply with the right to stop direct marketing and will amend this Policy accordingly.[3]

6.8.6 **Rights in relation to automated decision-making:** The right that a Data Subject has to receive information on and object to the processing of Personal Data using automated means where a decision is made by the Ministry that significantly affects the Data Subject, under certain conditions.[4]

At this time, the Ministry does not make any decisions based on the automated processing of Personal Data and recognizes that if it chooses to engage in automated decision-making in the future it must uphold the rights of Data Subjects and will amend this Policy accordingly.

6.8.7 **The right to complain:** Data Subjects have the right to complain to the Ombudsman and the Ministry about any perceived violation of the DPA by the Ministry. Complaints made directly to the Ministry shall be handled in the following manner:

i. The Ministry will ensure that there are processes in place to allow complaints to be received and resolved before escalation to the Ombudsman. The Data Protection Leader will lead on the response to a complaint from a Data Subject.
ii. Where complains from Data Subjects are received by employees of the Ministry, the complaint must be immediately reported to the Data Protection Leader who shall maintain an up-to-date log of complaints about any perceived violation of the DPA.
iii. The Data Protection Leader shall acknowledge receipt of the complaint within three (3) days of receipt.
iv. The complaint shall be referred to the Chief Officer and internal investigations undertaken by the Data Protection Leader on the direction of the Chief Officer.
v. A Report of the findings shall be made to the Chief Officer who will decide on the manner in which to proceed, consistent with the DPA.
vi. Steps should be taken internally to remedy the subject of the complaint.
vii. The Data Protection Leader shall notify the Data Subject within fourteen (14) days of the complaint on the outcome of the investigation and the steps taken to remedy the situation and confirm whether the issue has been rectified.
viii. The Data Protection Leader shall maintain an up-to-date log of complaints about any perceived violation of the DPA.

6.8.8 **The right to seek compensation:** The right to seek compensation through the Court when a Data Subject suffers damage due to a contravention of the DPA by the Ministry.[5]

[3]Under the DPA, "direct marketing" means communication, by whatever means, of any advertising, marketing, promotional or similar material, directed to particular individuals (i.e. using their personal data such as an email address). Most communication between Public Authorities and Data Subjects will not constitute "direct marketing".
[4] Under the DPA, a Data Subject is entitled to require a Data Controller ensure that no decision is taken that significantly affects the Data Subject based solely on automated processing of the Data Subject's Personal Data for the purpose of evaluating the Data Subject's performance at work, creditworthiness, reliability, conduct or any other matters relating to the Data Subject.
[5] Under Section 13 of the DPA, a Data Subject has a cause of action for compensation from the Ministry once damage is suffered as a result of the Ministry's breach of the DPA.

6.9 Data Subject Access Requests (DSARs)

This section represents the Ministry's Policy for identifying and treating with DSARs.

6.9.1 As part of the Ministry's day-to-day operations, an employee may receive DSARs from Data Subjects or their representatives seeking to exercise their rights under the DPA. Employees may also receive less formal, including verbal, requests for their Personal Data or information about why and how it is being processed by the Ministry.

6.9.2 In responding and/or processing DSARs, the Ministry will be guided by the DPA and the procedures within this Policy.

6.9.3 The Ministry will provide details of the following to Data Subjects, if a DSAR is made:

i. The Data Subject's personal data;
ii. The purposes for which they are being or to be processed by or on behalf of the Ministry;
iii. The recipients or classes of recipients to whom the data are or may be disclosed by or on behalf of the Ministry;
iv. Any information available to the Ministry as to the source of those personal data;
v. Any countries or territories outside the Cayman Islands to which the Ministry whether directly, or indirectly, transfers, intends to transfer or wishes to transfer the data;
vi. General measures to be taken or being taken against unauthorized or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

6.9.4 All DSARs received by employees of the Ministry shall be forwarded immediately to the Data Protection Leader, who also serves as the Information Manager.

6.9.5 The Information Manager will be responsible for handling DSARs in accordance with the DPA. The Ministry shall make reasonable efforts to process DSARs and grant the Data Subjects' requests to access their Personal Data and supplementary information without undue delay and within the timeframe required in the DPA.

6.9.6 The Information Manager, on the direction of the Chief Officer if necessary, will determine whether the Ministry reasonably requires further information in order to be satisfied as to the identity of the Data Subject making the request or to locate the information that the Data Subject seeks.

6.9.7 If more information is reasonable required, the Data Subject shall be informed in writing of the requirement.

6.9.8 The Ministry shall comply with a DSAR within thirty (30) days of the date on which the request was received. Provided however, that the time for responding may be extended for up to an additional thirty (30) days where:

i. A large amount of data is required or requested to be searched and meeting the timelines would unreasonably interfere with the Ministry's operations;
ii. More time is required to consult with a third party or other Data Controller in order for the Ministry to decide whether or not to give access to the Data Subject; or
iii. The Data Subject has given consent to the extension.

6.9.9 Where the Ministry requested further information the period shall not resume until the information has been supplied.

6.9.10 In complying with a DSAR, the Ministry shall, at all times, ensure that the personal data released, applies only to the individual making the request and that personal data of other persons are not disclosed in the response.

6.9.11 If the Ministry cannot comply with the DSAR without disclosing personal data relating to another Data Subject who can be identified from that personal data, the Ministry cannot comply with the request unless:

i. The other data subject has consented to the disclosure of the personal data, or
ii. It is considered reasonable in all the circumstances to comply with the request without the consent of the other Data Subject. Only the Chief Officer is authorized to decide how to proceed without this consent.

6.9.12 In determining whether it is reasonable to comply with the DSAR without the consent of the other Data Subject concerned, the Chief Officer shall have regard to:

i. Any duty of confidentiality owed to the other data subject;
ii. Any steps taken by the Ministry to seek the consent of the other Data Subject;
iii. Whether the other Data Subject is capable of giving consent; and any express refusal of consent by the other data subject

6.9.13 In providing the data through a DSAR, the Ministry will supply the data subject with a copy of the data requested in an intelligible form, and in the format requested unless:

i. the supply of such a copy is not possible or would involve disproportionate effort; or
ii. the data subject agrees otherwise.

6.9.14 If any of the personal data are expressed in terms that are not intelligible without explanation, the copy shall be accompanied by an adequate explanation.

6.9.15 Personal Data and other information supplied in furtherance of this section of the Policy shall be supplied by the Ministry by reference to the data in question at the time when the DSAR is received, except that regard will be had to any amendment or deletion made between that time and the time that the information is supplied, provided that the amendment or deletion is such that would have been made regardless of the receipt of the request.

6.9.16 Where the Ministry receives a DSAR, the Data Subject shall be informed of the right to complain to the Ombudsman under the DPA.

6.9.17 The Ministry will ensure that an up-to-date log of DSARs is maintained by the Information Manager and stored appropriately.

6.10 Data Accuracy

This section includes the measures that will be put in place to promote data accuracy. It describes the appropriate tools and processes for ensuring inaccurate personal data are not processed by the Ministry. Under the DPA, the Ministry is required to comply with the Data Protection Principle of data accuracy.

6.10.1 Through reasonable and appropriate verification measures, the Ministry shall ensure that the Personal Data it processes, particularly if it is to be used to make any decisions, is accurate, up-to-date and complete when considering the purpose(s) of the Processing.

6.10.2 The Ministry will carefully consider any challenges to the accuracy of Personal Data and implement processes and resources to rectify, block, erase or destroy inaccurate Personal Data and opinions based on inaccurate Personal Data without delay, including when ordered to do so by the Ombudsman following a complaint by a Data Subject.

6.10.3 If inaccurate Personal Data have been shared with Third Parties by the Ministry and are subsequently rectified, blocked, erased or destroyed, each Third Party shall be contacted and informed of the rectification – unless this proves impossible or involves disproportionate effort.

6.10.4 Any challenge to the accuracy of Personal Data received by the Ministry (where a complaint has not been made to the Ombudsman by the Data Subject) must be referred to the Data Protection Leader who shall launch an investigation and report the findings to the Chief Officer.

6.10.5 Upon receiving any technical input from the responsible Department, section, unit or statutory body concerned with the Personal Data, only the Chief Officer is authorized to decide whether the Personal Data is inaccurate and how to treat with rectification.

6.10.6 The Chief Officer upon considering all the circumstances, may give instructions to rectify, block, erase or destroy inaccurate Personal Data and opinions based on inaccurate Personal Data and the Data Protection Leader shall communicate these instructions to the Data Controller holding the inaccurate Personal Data.

6.10.7 Where necessary, the Chief Officer will consult with the Cayman Islands National Archives and/or the Solicitor General before giving instructions for rectification.

6.10.8 Where a complaint about Personal Data is being addressed through rectification, blockage, erasure or destruction of inaccurate Personal Data, the Data Protection Leader shall oversee that the process is being undertaken in accordance with sound records management practices as well as in conformity with the directives of the Chief Officer.

6.10.9 After the steps have been taken to address the complaint, the Data Protection Leader will report on the outcome to the Chief Officer and the Data Subject and any applicable third party will be advised accordingly.

6.10.10 The Ministry will aim to develop and maintain a Data Quality Policy to ensure that the highest standards of data quality are maintained and the roles and responsibilities of the Ministry's employees are defined to ensure that all data processed within its area of responsibility will be accurate, accessible and complete as far as is reasonably practical.

6.11 Security

6.11.1 The Ministry shall process Personal Data in a manner that maintains confidentiality, integrity and availability, considering the circumstances and risks of the processing and compliance with relevant local and international legislation and rules as well as contractual obligations. Appropriate physical, technical and organisational security measures shall be taken against unauthorised or unlawful processing of Personal Data, including to protect Personal Data from accidental loss, destruction or damage.

6.11.2 The Ministry shall adopt the **CIG Information Security Policy**.

6.11.3 The Ministry uses a range of physical, technical and organisational measures to safeguard Personal Data, including through our Data Processors. These measures include but are not limited to:

i. Developing and maintaining written plans to identify, prevent, detect, respond to, and recover from security threats, events and incidents;
ii. Developing robust authentication procedures for accessing all systems that store Personal Data;
iii. Administrative and technical controls to restrict access to Personal Data on a "need to know" basis;
iv. Maintaining systems, software and applications, anti-virus software, firewalls, and other computer security safeguards, and appointing appropriate personnel to be responsible for keeping such safeguards up to date.

v. Requiring Data Processors who process Personal Data on behalf of the Ministry to maintain appropriate security measures, including through MOUs, agreed Terms of Service or Data Processing Agreements;
vi. Maintaining appropriate records of access to and processing of Personal Data;
vii. Ensuring employees are trained on security policies and measures that have been implemented;
viii. Auditing security measures implemented to safeguard Personal Data at regular intervals, including when changes have been made to systems or processes and when legislative changes impact the processing of Personal Data, and recording the results of such audits;
ix. Using appropriate measures, such as encryption, pseudonymisation and chain of custody records, to protect Personal Data, including when stored on laptops, tablets, external hard drives, USB drives and other portable storage devices;
x. When applicable, utilising appropriate and secure methods to destroy Personal Data as legally required; and
xi. Taking all other reasonable measures as required from time to time by legislation, rules and policies.

6.12 Sharing Data with Joint Data Controllers, Data Processors and Third Parties

This section includes policy statements relating to the sharing of Personal Data with Joint Data Controllers, sharing Personal Data with Data Processors, and disclosure of Personal Data to Third Parties. The Joint Controller, Data Processor or Third Party may or may not be another Public Authority.

6.12.1 Prior to sharing Personal Data with a Joint Data Controller, or a Data Processor, or disclosing Personal Data to a Third Party, the Ministry shall ensure that the proposed processing complies with the Data Protection Principles[6] and other requirements of the DPA, including the requirement to identify a legal basis or legal bases for the processing. See also **Legal Bases/Conditions of Processing** (section 6.5).

6.12.2 The Ministry will ensure that its Data Processors comply with the Data Protection Principles when processing Personal Data on behalf of the Ministry or any other Public Authority as the Data Controller.

6.12.3 The Ministry will ensure all parties have sufficient clarity in relation to data protection roles, responsibilities and requirements – including through the establishment of appropriate written contractual or similar measures[7] via MOU, Terms of Service or Data Processing Agreement – when any of the following situations occur:
   a. The Ministry, as a Data Controller, uses a Data Processor to process Personal Data;
   b. The Ministry, acting as a Data Processor, engages another Data Processor (i.e. Sub-Processor);
   c. The Ministry and one or more other Data Controllers are identified as Joint Data Controllers; and/or

[6] Schedule 1 of the DPA
[7] Section 7.12 of the **CIG Privacy Policy** requires the roles of each Public Authority to be "clearly established" where two or more Public Authorities Process Personal Data in order to deliver a public policy, service or programme.

d. The Ministry as a Data Controller regularly discloses Personal Data to a Third Party, including another Public Authority.

6.12.4 Where the Ministry engages a Data Processor, the terms and conditions of the sharing of Personal Data shall be documented in an MOU (between Public Authorities), in Terms of Service that have been established by the Data Processor (where one Public Authority acts as a Data Processor for two or more other Public Authorities) and agreed by all Data Controllers, or in a Data Processing Agreement (between a Public Authority and a non-CIG Data Processor).

6.12.5 The Ministry shall ensure that all Data Processors providing services mentioned in this section are contractually required to follow the policies set forth herein, or substantially equivalent standards, and to protect Personal Data in accordance with the applicable legal framework and subject to any appropriate security measures and directions from the Ministry. These requirements should also apply to any subcontractors that may be engaged by the Data Processor.

6.12.6 Prior to disclosing Personal Data to a Third Party, the Ministry will ensure the proposed disclosure complies with the Data Protection Principles and other requirements of the DPA, including the requirement to identify a legal basis or legal bases for the disclosure.

6.12.7 The Ministry will aim to develop and maintain a Data Processor Management Policy which details requirements for control over Data Processors that use the Ministry's information systems.

6.12.8 Where applicable, the Ministry will aim to develop a Data Sharing Policy to ensure the efficient and effective sharing of Personal Data, particularly with other Public Authorities.

6.13 International Transfers

Personal Data may be transferred outside of the Cayman Islands to another country or territory only when the receiving country or territory ensures an adequate level of protection for the rights and freedoms of Data Subjects in relation to the processing of Personal Data.

6.13.1 The Ministry shall refrain from transferring Personal Data to countries or territories that do not have adequate protections for Personal Data. This means that the Ministry will only transfer Personal Data to a Person, including a Data Processor, that is located in a country or territory that ensures an adequate level of protection for the rights and freedoms of Data Subjects in relation to the processing of Personal Data, unless an exception under Schedule 4 of the DPA applies[8]

6.13.2 The Ministry shall ensure that measures are in place to ensure that an appropriate MOU (used between Public Authorities) or Data Processing Agreement (used with external suppliers and service providers) is executed with a Data Processor or that appropriate Terms of Service (for Public Authorities that serve as Data Processors for multiple Public Authorities) have been agreed by the Data Controller(s) before Personal Data are transferred internationally to that Data Processor, and that such contracts or other governing documents contain appropriate data protection clauses.

6.13.3 The Ministry shall ensure that if Personal Data may be transferred to a Recipient, including a Data Processor, located outside the Cayman Islands, measures are in place for the design, adoption and implementation of appropriate international data transfer

[8] See CIG Privacy Policy Appendix D: International Transfers for more details.

mechanisms prior to the transfer to ensure that Personal Data that are or may be transferred internationally are adequately protected.

6.13.4 Where appropriate, the Ministry shall incorporate any standard contractual clauses published and/or approved by the Ombudsman in MOUs, Terms of Service or Data Processing Agreements that include or may require the international transfer of Personal Data.

6.14 Incident Reporting and Response

This section includes policy statements that must be implemented in order to respond to real or suspected security incidents where Personal Data are involved.

A personal data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of or, access to, personal data transmitted, stored or otherwise processed

6.14.1 Personal data breaches can be the result of both accidental and deliberate causes and can include:

i. Access by an unauthorized third party
ii. Deliberate or accidental action (or inaction) by a Data Controller or Data Processor
iii. Sending personal data to an incorrect recipient
iv. Lost or stolen computing/digital devices containing personal data
v. Loss of availability of personal data, including through a technical fault.

6.14.2 There are different types of security incidents that can lead to personal data breaches which can affect the following aspects of personal data:

i. Confidentiality, for example, unauthorized disclosure of personal data to a third party by directing an email to the wrong person.
ii. Integrity, for example, where personal data such as dates of birth were changed in a spreadsheet and are no longer accurate.
iii. Availability, for example, paper application forms were shredded before they had been scanned into an electronic database.

6.14.3 The Ministry shall ensure that any suspected theft, loss or unavailability of Personal Data, other unauthorised processing of Personal Data, or damage to Personal Data is immediately investigated.

6.14.4 The Ministry shall take steps to immediately examine the cause of a security-related event and make efforts to contain any incidents or breaches and mitigate any risk of harm.

6.14.5 All Ministry personnel must immediately report all suspected personal data breaches to their Manager and/or Data Protection Leader. Only the Chief Officer or designate is empowered to confirm, with relevant information, and through consultation with subject matter experts, if necessary, whether a personal data breach has occurred.

6.14.6 The Chief Officer or designate such as the Data Protection Leader will take steps to immediately investigate any security or privacy related incident and make every effort to contain any breach and mitigate the risk of harm that may result from the breach. In doing so, all personal data breaches must be specifically assessed to determine if the breach is likely to prejudice the rights and freedoms of the affected data subject(s). All connected Ministry employee shall assist with an investigation if required.

6.14.7 Until a personal data breach has been declared by the Chief Officer or designate, any suspected breach should be considered a security incident. During this time, all

communication should be internal until the Data Protection Leader is authorized by the Chief Officer to effect external Notifications pursuant to the DPA.

6.15 Personal Data Breach Notification

6.15.1 Where the Chief Officer has decided that a personal data breach has occurred, the Ministry will, within no more than five (5) days of becoming aware of the personal data breach, notify the Data Subject and the Ombudsman of the breach.[9]

6.15.1 The Data Protection Leader or other personnel so authorized by the Chief Officer will lead on these notifications. When notifying data subjects, the Ministry should provide the information in a clear, approachable and intelligible way. Notifications should be professional, demonstrate accountability, and make best efforts to maintain and/or regain the trust of the Data Subject.

6.15.2 The Data Protection Leader shall, under the direction of the Chief Officer, report Personal Data Breaches to the Ombudsman and to impacted Data Subjects in line with the requirements of the DPA. Notifications shall be provided without undue delay and those Notifications to the Data Subjects shall describe, at minimum[10]:

i. the nature of the breach;
ii. the consequences of the breach;
iii. measures taken or proposed to be taken by the Ministry to address the breach; and
iv. measures recommended by the Ministry to the Data Subject to mitigate the possible adverse effects of the breach.

6.15.3 The Ombudsman has issued a form to report personal data breaches which will be used in all instances of personal data breaches. The form can be found on the Ombudsman website at: https://oci-webform.workpro-online.com/Client/complaints. This form should only be submitted by the Data Protection Leader after the Chief Officer has determined that a data breach has occurred[11]

6.15.4 If the Ministry uses a Data Processor, the requirements on reporting a breach should be detailed in the contract for services[12]

6.15.5 If the Ministry uses a Data Processor who suffers a reportable breach involving personal data processed on behalf of the Ministry as the Data Controller, then the Ministry- as the Data Controller- must inform the Ombudsman, and the data subject without delay and always within the five-day reporting period.

6.15.6 In the context of data breaches, the Ministry will exercise due diligence which means that systems will be managed on an on-going basis and monitored for any accidental or deliberate destruction, loss, alteration, unauthorised disclosure of or, access to, the personal data processed.

6.15.7 The Ministry will prioritize the investigation of a potential breach, give it adequate resources, and expedite it urgently. If it is not possible to investigate a breach fully within 5 days to understand exactly what has happened and what needs to be done to mitigate it, the Ministry will provide the additional information to the Ombudsman as soon as possible without undue further delay. If full details cannot be provided within

[9] Data Protection Act, (2021 Revision), Section 16(1)

[10] The Personal Data Breach Notification Template is appended to this Policy.

[11] This form is to be used for reporting Personal Data Breaches to the Ombudsman

[12] See the Seventh Data Protection Principle, Schedule 1, Part 1 of the DPA

the 5 days, the Ombudsman will be notified and an explanation and timeframe for submission provided.

6.15.8 The Data Protection Leader shall maintain a record of all Personal Data Breaches, including:

i. the nature of the breach;
ii. likely consequences of the breach for Data Subjects;
iii. categories of Data Subjects concerned;
iv. types and amount of Personal Data involved;
v. the cause of the incident (if known);
vi. how the breach was identified;
vii. the date and time the breach occurred (if known);
viii. the location and duration of the incident;
ix. the date and time the breach was identified;
x. if the breach occurred at a Data Processor, the identity of the Data Processor;
xi. remedial actions proposed to be taken to address the breach;
xii. remedial actions taken to address the breach;
xiii. when the breach was reported to the Ombudsman and to affected Data Subjects; and
xiv. when the case was closed.

6.16 Data Retention and Disposal

This section includes policy statements on the retention and disposal of Personal Data for the Ministry and applicable requirements in which Personal Data can be destroyed. Under the DPA, the Ministry is obliged to comply with the Data Protection Principle of storage limitation.

6.16.1 The Ministry shall only retain Personal Data for as long as it is needed and in compliance with the legal obligation to create, manage, maintain and dispose of public records under the National Archive and Public Records Act (2015 Revision) and/or any other applicable legislation or legal obligation.

6.16.2 The Ministry will adhere to its Data Retention Policy and relevant disposal schedules which set out minimum retention periods.

6.16.3 The Ministry shall securely destroy or erase Personal Data from its systems and physical documents when it is no longer required to accomplish the purpose for which it was collected or to comply with legal obligations, including the obligation to maintain and/or archive public records.

6.16.4 When the Ministry securely deletes and destroys Personal Data that are no longer required, every effort will be made to ensure the same Personal Data maintained by Joint Data Controllers and Data Processors are also securely deleted and destroyed. This requirement does not apply where Joint Data Controllers and Data Processors may need to retain (some or all) Personal Data in order to comply with applicable laws or court orders.

6.16.5 The Ministry shall align retention policies and disposal schedules with the DPA, **CIG Privacy Policy** and other applicable policies and framework.

6.16.6 The Ministry shall either de-identify, anonymise, secure or destroy Personal Data when the Personal Data are no longer required for a specific purpose to mitigate the risk of a Personal Data Breach.

6.17 Acting as a Data Processor

The Ministry will be considered a Data Processor in the rare event of processing Personal Data on behalf of a Data Controller, which may be a separate Public Authority. In this capacity, the main data protection responsibilities of the Ministry acting as a Data Processor are:

6.17.1 Ensuring that an MOU or Data Processing Agreement is in place with the Data Controller(s) or that the Ministry has established clear Terms of Service that have been agreed with the Data Controller(s);
6.17.2 Ensuring that all activities and tasks of the Ministry are carried out as agreed in the MOU, Terms of Service or Data Processing Agreement;
6.17.3 Maintaining a RoPA or other Personal Data inventory or map if required to do so, including as per the MOU, Terms of Service or Data Processing Agreement. See also **Data Inventory, Data Mapping and Record of Processing Activities (RoPA)**;
6.17.4 Implementing appropriate security measures to protect the Personal Data processed by the Ministry on behalf of the Data Controller;
6.17.5 Informing the Data Controller in the event of a Personal Data Breach within the stipulated timeframe outlined in the MOU, Terms of Service or Data Processing Agreement; and
6.17.6 If clearly and solely responsible as per the MOU, Terms of Service or Data Processing Agreement, informing the Ombudsman of Personal Data Breaches within the stipulated timeframe(s), subject to any exemptions that may apply.

6.18 Exemptions

In limited circumstances, the Ministry will carefully consider the circumstances in which exemptions apply to its processing activities and shall only apply such exemptions in accordance with the DPA[13]. Only the Chief Officer is authorized to determine whether an exemption applies having obtained subject matter and legal advice as necessary.

6.19 Training and Awareness

6.19.1 The Ministry shall ensure that all employees and other Public Officials who handle or have access to Personal Data on its behalf are aware of their responsibilities under this Policy and other relevant data protection and information security policies and procedures.
6.19.2 All employees of the Ministry, Department of Education Services and the Cayman Islands Public Library Service shall receive data protection training at least annually or when there are significant changes to the processes and/or to this Policy. Public Officials who handle or have access to Personal Data, including members of boards and committees, shall receive data protection training as soon as practicable after their appointment or engagement and at appropriate intervals thereafter.
6.19.3 The Ministry shall ensure that its employees receive and attend the required data protection training, including the content and handling of this Policy and any additional data protection training specific to their role, if they have access to Personal Data.
6.19.4 All Recipients of Personal Data Processed by the Ministry shall be made aware of both their individual responsibilities and of the Ministry's responsibilities under the DPA and under this Policy.

[13] See Part 4 of the DPA for the complete list of Exemptions.

6.19.5 The Ministry shall ensure that all its employees receive and attend training to identify DSARs and other requests or notices where Data Subjects are seeking to exercise other rights, and how to respond or forward the request or notice to the Information Manager or Data Protection Leader. See also **Individual Rights** (section 6.8).

7 DATA PROTECTION LEADER

The Ministry has appointed a Data Protection Leader to oversee implementation, enforcement and maintenance of this Policy and to carry out the duties as set out in the **CIG Privacy Policy**. The DPL will be adequately resourced and will report to the Chief Officer in relation to their DPL responsibilities. The DPL also serves as the Information Manager for the Ministry.

The DPL's primary responsibilities will include:

i. Monitoring internal compliance with this Policy, and the obligations under the Data Protection Act and Regulations and the CIG's Privacy Policy;
ii. Informing and advising on data protection obligations under the DPA, Regulations and the CIG's Privacy Policy;
iii. Providing advice regarding DPIAs;
iv. Acting as a contact point for Data Subjects; and
v. The functions highlighted in Table 5 above.

If you have any questions about this Policy or how Personal Data are handled, or if you need to report an actual or suspected Personal Data Breach or communication from a Data Subject regarding Data Subject Rights, please contact the Data Protection Leader.

Name: Stacy-Ann Dewar
Phone Number: 244-2483
Email Address: stacy-ann.dewar@gov.ky
Address: Government Administration Building| 133 Elgin Avenue| Grand Cayman KY1-9000

8 POLICY EVALUATION AND CHANGE

Any employee of the Ministry or other Public Official may recommend changes to this Policy through their manager or directly to the Data Protection Leader.

This Policy will be formally reviewed by the Data Protection Leader, under the direction of the Chief Officer and in consultation with the senior management team for its completeness, adequacy, and alignment to the Ministry's functions and priorities at least annually, and on a more frequent basis if deemed necessary. All employees will support the review of this Policy, as required.

All substantive amendments of this Policy will be approved by the Chief Officer.

APPENDICES[14]

1) Data Inventory and Mapping Template
2) Data Protection Impact Assessment Template
3) External Privacy Notice
4) Suspected Breach Report Form
5) Personal Data Breach Notification Template

[14] The Templates referenced in this Policy have been issued by the Information Rights Unit of the Cayman Islands Government Cabinet Office in conformity with the CIG Privacy Policy.

DATA INVENTORY AND MAPPING TEMPLATE

A quick review – what is the current position	**Response** Yes/No/Being implemented
Senior management awareness • Regularly discuss data protection • Data protection has been identified as a compliance issue	
Data protection policies and procedures (including retention and disposal schedules, internal practical guidance for staff to follow with regard to the processing of personal data by the controller) • in place • communicated to staff • compliance is monitored • compliance can be evidenced • regularly reviewed	
Information security **Policies and procedures:** • in place • communicated to staff • compliance is monitored • compliance can be evidenced • regularly reviewed **Formal mechanisms in place to identify breaches and handle incidents** • in place • communicated to staff • compliance is monitored • compliance can be evidenced • regularly tested & reviewed	
Clear and accessible fair processing information given to individuals	
New projects and initiatives • "privacy-proofed" at the planning stage • Reviewed during development, testing and delivery stage, i.e. pre- and post-implementation • 'Privacy impact assessments' are conducted when necessary	

WHY is personal data processed? **List the reasons for processing**

You will need to complete this page for <u>each reason</u> for processing
WHOSE personal data is processed?
Reason for processing:

You will need to complete this page for <u>each reason</u> for processing

WHAT personal data is processed?		**Reason for Processing:**
Type of personal data	**Source**	**Legal Bases** **Schedules 2 and 3 of the Data Protection Act as applicable**

You will need to complete this page for each reason for processing	
WHERE is personal data processed?	
Reason for Processing:	
Manual records location	
Electronic records format(s)	
Systems/services used	

DATA PROTECTION IMPACT ASSESSMENT[15]

DATA CONTROLLER DETAILS

Data Controller.	
Data Controller Main Contact	
Data Protection Leader/equivalent	

STEP 1: IDENTIFY THE NEED FOR A DPIA

Explain broadly what the project aims to achieve and what types of processing it involves.

STEP 2: DECRIBE THE (PROPOSED) PROCESSING OF PERSONAL DATA

2.1 Describe the purpose(s) of the processing.

[15]For processing activities that are unlikely to present a high risk to data subjects, a less detailed "screening" may be appropriate to document the level of risk and justify why a DPIA has not been conducted. This Form has been developed by the Information Rights Unit based on a similar template issued by the United Kingdom's Information Commissioner's Office.

2.2 Where and how will the personal data be obtained?
2.3 How will the personal data be used and stored once it has been collected?
2.4 What types of personal data will be processed? Does this include any sensitive personal data?
2.5 Will the personal data be shared with anyone?
2.6 How many data subjects are affected? How often will the Ministry be processing the personal data?
2.7 How long will the Ministry keep the personal data? Are the public records included in a disposal schedule?
2.8 Will any personal data be transferred outside of the Cayman Islands?
2.9 What is the nature of the Ministry's relationship with the data subjects? How much control will they have over the processing? Would these data subjects expect the Ministry to use their personal data in this way?
2.10 Do these data subjects include children or other vulnerable groups?

2.11 Are there prior concerns over this type of processing or security flaws? Is it novel in any way? Does it involve emerging technology? Are there any current issues of public concern that should be factored in?
2.14 Is the Ministry signed up to any code of conduct or certification scheme relevant to the processing?

STEP 3: CONSULTATION

3.1 What are the views of the data subjects and other impacted individuals?
3.2 What information or feedback has the Ministry received from other relevant parties?

STEP 4: ASSESS NECESSITY AND PROPORTIONALITY

4.1 What is/are the Ministry's conditions for processing the personal data? *Schedules 2 & 3 to the Data Protection Act.*
4.2 How does the processing actually achieve the Ministry's purpose?
4.3 Is there another way to achieve the same outcome, i.e. without processing the personal data at all, or by processing less personal data, or by processing personal data in a less invasive way?

4.4 Has the Ministry considered all purposes for processing the personal data as well as other potential "uses" that are not directly relevant to its aims? How will function/scope creep be prevented?
4.5 How will the Ministry ensure data quality (i.e. data accuracy) and data minimisation?
4.6 What information will data subjects be given about the Ministry's processing activities? When? How?
4.7 How will the Ministry help to support and facilitate data subject rights under the Data Protection Act?

STEP 5: IDENTIFY AND ASSESS RISKS

Describe each risk, including the source and nature of its potential impact on individuals. *Include risks to individuals and the Ministry*	**Likelihood of harm** *(remote, possible or probable)*	**Severity of harm** *(minimal, significant or severe)*	**Overall risk** *(low, medium or high)*
a) *[Describe each risk here in sufficient detail]*			
b)			
c)			

STEP 6: IDENTIFY MEASURES TO REDUCE RISK

6.1 Identify the technical, physical and administrative measures the Ministry could take to address these risks. *For risks identified as being medium/high overall and not remote.*				
Risk	**Measure to address the risk**	**Effect on the risk**	**Residual risk if implemented**	**Measure approved (If applicable)**
[Reference by letter / summarise the risk(s) from Step 5 here]		*[eliminated / reduced]*	*[none / low / medium / high]*	*[yes / no]*
6.2 What measures will be taken to ensure any data processors comply with the Data Protection Act? C*ontract / MoU / Terms of Service to be implemented.*				
6.3 How will the Ministry safeguard any international transfers, is applicable?				

STEP 7: SIGN OFF AND RECORD OUTCOMES

Item	**Name, position, date completed**	**Notes**
Measures to reduce risk approved by:		
Residual risks accepted by:		
Data Protection Leader (DPL)/subject matter expert		

who provided advice:		
Advice [accepted / overruled] by:		
Consultation responses reviewed and considered by:		
Summary of data protection advice:		
Comments on data protection advice:		
Comments on consultation responses:		

DPIA Version Number:		Version Date:		Review Date:	
DPIA will kept under review by:					

PRIVACY NOTICE

External Privacy Notice

1. Scope

The Ministry of Education, the Department of Education Services and the Cayman Islands Public Library Services. ("the Ministry") respects your privacy and take care in protecting your personal data. As a data controller, we comply with the Cayman Islands Data Protection Act (2021 Revision) (the "DPA"). This privacy notice ("Privacy Notice") demonstrates our commitment to ensuring your personal data is handled responsibly and applies to the processing of personal data undertaken by the Ministry in fulfilling our mandate.

2. What Personal Data We Collect

The Ministry collects personal data, including sensitive personal data, directly from you and may also collect your personal data indirectly from third party sources. Personal data collected by the Ministry is limited to what is necessary for our processing activities.

Personal data we collect directly from you

The Ministry collects the following information directly from you:

i. Personal data you provide through the Ministry's websites, such as details provided within comments and questions, including your name and/or email address if you provide these details in our web form. If you ask questions about our public services and programmes or provide information about your relationship with us, this may also reveal other personal data;
ii. Personal data you provide when you visit the Ministry's offices and other locations, contact us by email or telephone, or access our programmes and services, including our online application and registration portals;
iii. Personal data that you provide when you inquire about or apply for a job with the Ministry;
iv. Personal data collected via CCTV at the Ministry's premises, including images via cameras located at
    a. The Government Administration Building- 133 Elgin Avenue;
    b. The Department of Education Services- 130 Thomas Russell Avenue, PO Box 910. George Town; and
    c. The Cayman Islands Public Library Services- 68 Edward Street George Town
v. Any information you choose to provide when interacting with the Ministry on social media platforms, including:
    a. Facebook;
    b. Instagram;
    c. LinkedIn; and
    d. YouTube

Personal data collected from other sources

The Ministry may collect Personal Data from other sources including:

i. Third Parties that verify Personal Data that you provide to the Ministry;
ii. Third Parties that share employment and other information for authentication purposes;
iii. Other entities within the Cayman Islands Government; and
Third Parties that support the Ministry in the processing of Personal Data in the exercise of public functions.

3. How We Use Your Personal Data

The purpose of the Civil Service is to make the lives of those we serve better. We are dedicated to supporting the elected government by delivering caring, modern and customer-centred public services and programmes, which deliver value for money. The Ministry may use your personal data for the following purposes:

i. Implementing policies, providing services and programmes, and managing your relationship with us;
ii. Responding to your inquiries;
iii. Verifying your identity and other information provided;
iv. To determine eligibility for funding programmes offered by the ministry;
v. Measuring how users interact with the Ministry's online portals and continually improving our communications channels (including by aggregating personal data collected using cookies);
vi. Communicating and interacting with you;
vii. Communications and public relations activities;
viii. Managing accounts payable and receivable, preventing fraud, and protecting public funds;
ix. Statistical and other reporting, both internally and externally;
x. Seeking legal advice, and exercising or defending legal rights;
xi. Complying with our legal obligations, including all legislation that applies across the public sector; and
xii. Communicating and interacting with job applicants and related third parties (e.g. references) and carrying out recruitment and selection processes.

4. How We Share Your Personal Data

The Ministry may share your personal data as required, including under applicable legislation, with recipients that include joint data controllers, our data processors, and third parties. We will only share your personal data as permitted by the Cayman Islands DPA.

Your personal data may be shared with the following recipients that support our public functions and operations:

i. **With other public authorities:** Personal data may be shared with other public authorities being Ministries, Portfolios, Offices, Departments, Statutory Authorities, Statutory Bodies and Government Companies for the purposes set out in this Privacy Notice.
ii. **With data processors external to the CIG:** Personal data may be shared with persons providing services to the Ministry as a data processor in compliance with the Cayman Islands DPA. These service providers are only able to use personal data under our instructions and may include:
    a. Webhosting;
    b. Information Technology;

c. Records and Information Management, including storage facilities;
d. Communications;
e. Security operations and fraud prevention.

iii. **With legal advisors and other persons if required by law or in relation to legal proceedings or rights:** Personal data may be disclosed as legally required, for the purpose of or in connection with proceedings under the law, if necessary to obtain legal advice, or if the disclosure is otherwise necessary to establish, exercise or defend legal rights. This may include disclosing your personal data for the following purposes:
   a. Seeking legal advice;
   b. Exercising or defending legal rights;
   c. Complying with internal and external audits or investigations by competent authorities;
   d. Complying with information security policies or requirements; and

5. Our Legal Bases for Processing Your Personal Data

Depending on applicable laws and other circumstances, the Ministry will rely on specific legal bases, or "conditions of processing", under the Cayman Islands DPA to process your personal data. These may include:

i. A **legal obligation** to which the Ministry is subject, and to comply with various obligations under the Education Law 2016, the Education Regulations 2017, the Children Law (2012 Revision) and all other applicable laws under the CIG Framework.
ii. To exercise **public functions**, including registration of all educational institutions and providing policy advice, administrative and governance support and the delivery of a range of programmes and services to the public that enable the CIG to achieve the strategic goals for Education.
iii. To perform or enter into a **contract** with you, such as for the provision of goods and services;
iv. **Consent**, in order to send you marketing communications or to administer surveys and polls; and
v. For the purposes of **legitimate interests** pursued by the Ministry or by a third party or parties to whom the personal data may be disclosed.

Where we process your sensitive personal data, we will also meet a second legal basis. These may include:

i. To exercise our **public functions**; and
ii. In relation to **legal proceedings**, including obtaining legal advice and otherwise establishing, exercising or defending legal rights.

6. Children's Personal Data

The Ministry collects personal data relating to children under the age of 18 to enable us to deliver public services and programmes and carry out our functions. We may collect children's personal data for any of the purposes set out in section 3 of this Privacy Notice, in addition to:

i. Determining eligibility for funding under the Early Childhood Funding Programme (ECAP);
ii. Processing applications for and awarding government scholarships;
iii. Administering the School Meals Programme; and

iv. To determine Additional Learning Support Needs across educational institutions

7. Security and International Transfers

The Ministry has put in place appropriate technical, physical and organisational measures in order to keep your personal data secure. These safeguards to maintain the confidentiality, integrity and availability of your personal data may include:

i. Developing and maintaining written plans to identify, prevent, detect, respond to, and recover from security threats, events and incidents;
ii. Developing robust authentication procedures for accessing all systems that store Personal Data;
iii. Maintaining systems, software and applications, anti-virus software, firewalls, and other computer security safeguards, and appointing appropriate personnel to be responsible for keeping such safeguards up to date.
iv. Requiring Data Processors who process Personal Data on behalf of the Ministry to maintain appropriate security measures, including through MOUs, agreed Terms of Service or Data Processing Agreements;
v. Ensuring employees are trained on security policies and measures that have been implemented;
vi. Auditing security measures implemented to safeguard Personal Data at regular intervals; and
vii. Using appropriate measures, such as encryption, pseudonymisation and chain of custody records to protect Personal Data.

The Ministry will not transfer personal data to countries or territories that do not ensure an adequate level of protection for personal data. We may transfer your personal data outside of the Cayman Islands to Canada and the United Kingdom where data are stored securely by our IT service providers.

We will only transfer your personal data to a country or territory that ensures an adequate level of protection for your rights and freedoms in relation to the processing of your personal data, unless there is a relevant exemption or exception under the Cayman Islands DPA. Exceptions may include your consent or appropriate safeguards.

8. How Long We Keep Your Personal Data

The Ministry may store your personal data for as long as we need it in order to fulfil the purpose(s) for which we collected your personal data, and in line with any applicable laws. This includes the National Archive and Public Records Act (2015 Revision), which governs the creation, maintenance and disposal of all public records. Sometimes, we may anonymise your personal data so that it is no longer associated with you.

9. Cookies

Cookies, in combination with pixels, local storage objects, and similar devices (collectively, "Cookies"), are used to distinguish between visitors to a website.

When you visit the Ministry's website, small files known as Cookies may be stored on your computer, phone, tablet or any other device through your web browser. Information is stored in these text files.

Enabling Cookies may allow for a more tailored browsing experience and is required for certain website functionality. In the majority of cases, a Cookie does not provide us with any of your personal data.

10. Your Rights

The Ministry will respect and honour your rights in relation to your personal data and implement measures that allow you to exercise your rights under the DPA and other applicable legislation.

In accordance with the DPA, your rights in relation to your personal data include:

i. **The right to be informed and the right of access:** The right to request access to all personal data the Ministry maintains about you as well as supplementary information about why and how we are processing your personal data. This is commonly known as a Subject Access Request and certain supplementary information about our processing is contained within this Privacy Notice.

ii. **Rights in relation to inaccurate data:** The right to request the rectification, blocking, erasure or destruction of any inaccurate personal data the Ministry maintains on you. We will ensure, through all reasonable measures, that your personal data is accurate, complete and, where necessary, up-to-date, especially if it is to be used in a decision-making process.

iii. **The right to stop or restrict Processing:** The right to restrict or stop how the Ministry uses your personal data in certain circumstances.

iv. **The right to stop direct marketing:** The right to cease the use of your personal data by the Ministry for direct marketing purposes. The Ministry does not currently carry out any direct marketing activities. However, we will update this Privacy Notice and we will also notify you in writing as required if this position changes.

v. **Rights in relation to automated decision making:** The right to obtain information about and object to the use of automated decision making by the Ministry using your personal data. The Ministry does not currently use automated means to make decisions about you. However, we will update this Privacy Notice and we will also notify you in writing as required if this position changes.

vi. **The right to complain:** The right to complain to the Ombudsman about any perceived violation of the DPA by the Ministry.

vii. **The right to seek compensation:** The right to seek compensation in the Court if you suffer damage due to a contravention of the DPA by the Ministry.

You may contact the Ministry, using the contact details listed below, to access and review your personal data or to exercise any other rights provided to you under the DPA. The Ministry will take into consideration circumstances where, under the DPA or other applicable legislation, your rights may be limited or subject to conditions, exemptions or exceptions.

Upon contacting the Ministry, we may need to verify your identity prior to fulfilling a request

and may request additional information as required. In accordance with the DPA, the Ministry may also charge a reasonable fee in relation to your request if it is unfounded or excessive in nature, or the Ministry may reserve the right not to comply with the request at all.

To learn more about your rights, visit www.ombudsman.ky.

11. Data Protection Principles

When processing your personal data, the Ministry will comply with the eight Data Protection Principles defined within the Cayman Islands DPA:

i. **Fair and lawful processing:** Personal data shall be processed fairly. In addition, personal data may be processed only if certain conditions are met, for example the data controller is subject to a legal obligation that requires the processing or the processing is necessary for exercise of public functions.

ii. **Purpose limitation:** Personal data shall be obtained only for one or more specified, explicit and legitimate purposes, and not processed further in any manner incompatible with that purpose or those purposes.

iii. **Data minimisation:** Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are collected or processed.

iv. **Data accuracy:** Personal data shall be accurate and, where necessary, kept up-to-date.

v. **Storage limitation:** Personal data processed for any purpose shall not be kept for longer than is necessary for that purpose.

vi. **Respect for the individual's rights:** Personal data shall be processed in accordance with the rights of data subjects under the DPA, including subject access.

vii. **Security – confidentiality, integrity and availability:** Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

viii. **International transfers:** Personal data shall not be transferred to a country or territory unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

12. How to Contact Us

The Ministry has appointed a Data Protection Leader. If you have any questions about this Privacy Notice or how your personal data is handled, or if you wish to make a complaint, please contact:

Name: Data Protection, Information and Records Manager
Telephone number: (345) 244-2483

Email Address: @gov.ky
Address: Government Administration Building, 133 Elgin Avenue, Box 108, Grand Cayman

The ministry aims to resolve inquiries and complaints in a respectful and timely manner.

13. Changes to this Privacy Notice

The Ministry reserves the right to update this Privacy Notice at any time and will publish a new Privacy Notice when substantial updates are made. From time to time, the Ministry may also notify you about the processing of your personal data in other ways, including by email or through our publications.

This Privacy Notice was last updated on _____.

SUSPECTED DATA BREACH REPORT

Part 1: Initial Internal Report of Security Incident Involving Personal Data ***This part is to be completed by the public official who discovered the incident or by the public official who has the most information about the incident.*** Completing this part may require consulting other individuals to obtain as much information as possible about the incident. If any information is unknown at this time, note this in your report and, if possible, indicate when it may be available. Your personal data may be used to follow up with you if necessary. All civil servants and other public officials (including members of boards, committees, etc) must **immediately** report security incidents involving personal data to their manager and/or Data Protection Leader, as appropriate. Any queries from data subjects or other persons must be referred to the Data Protection Leader. Unless directly authorised to do so by your Data Protection Leader, Chief Officer or Head of Department, **you must not** answer questions about security incidents; confirm, imply or deny that a personal data breach has occurred; or contact/notify the Ombudsman or affected data subjects.	
Date and time incident began	
Date and time incident discovered	
Date and time incident contained	
Where the incident occurred (i.e. the physical or digital location and systems or processes affected)	
Description of the incident (e.g. the nature of the incident, how it was discovered, what caused it)	
Number of individuals affected and their relationship to the agency	
Personal data impacted by incident (e.g. types/categories, volume)	
How the incident was discovered and any actions taken in response	
Please provide any additional information that may be relevant (e.g. if any external party is aware of the incident, involvement of any service providers, communication with the Ombudsman, if any critical services are currently down, etc.)	
Your name, title and department	

Your contact details	
Date and time Part 1 sent to Data Protection Leader	

Part 2: Investigation of Security Incident Involving Personal Data

This part is to be completed by the Data Protection Leader for the relevant Data Controller.

If more than one Data Controller is impacted, the Data Protection Leaders must consult each other to determine who will lead the investigation, with the other Data Protection Leaders assisting as required. Alternatively, if more appropriate, this form may be sent to each Data Protection Leader to separately investigate the incident from the perspective of the Data Controller for whom they are responsible.

Name, title and department of Data Protection Leader	
Date and time Part 1 received	
Data Controller(s) for the personal data affected by the incident (and relationship if multiple Controllers)	
Data Processor(s) involved	
Additional information obtained during the investigation (include any information that completes or corrects what has been provided in Part 1 but do not edit that section directly in order to maintain the integrity of the original report)	
Measures already taken to address the incident and/or mitigate its effect	
Assessment of incident, i.e. in your view, does this constitute a personal data breach and why or why not	
Further measures proposed to be taken to address the incident and/or mitigate its effect (if any)	
If the incident is a breach, measures recommended for data subject(s) to mitigate possible adverse effects	
Date and time Parts 1-2 sent to Chief Officer/Head of Department	

Part 3: Declaration on Security Incident Involving Personal Data ***This part is to be completed by the (Acting) Chief Officer or (Acting) Head of Department.*** Under the CIG Privacy Policy, only the Chief Officer/Head of Department is able to confirm, with relevant information and advice, whether a personal data breach has occurred. Until a personal data breach has been declared, any suspected personal data breach is to be considered a security incident. If a personal data breach is declared, the Data Protection Leader will manage the response and lead on all notification and reporting requirements, unless explicitly instructed otherwise. The Chief Officer/Head of Department may assign some or all of these tasks to another individual, e.g. the Process Owner, by providing detailed instructions in this document. If response tasks are split among multiple individuals, the Data Protection Leader will coordinate activities and be responsible for completing Part 4.	
Name, title and department of relevant Chief Officer/Head of Department	
Date and time Parts 1-2 received	
Based on the assessment of the Data Protection Leader in Part 2, does this incident constitute a personal data breach or not? If you disagree with the assessment, please explain why	
Comments or instructions to Data Protection Leader and/or any other public official in relation to the incident/breach and the response, e.g. whether to proceed with the measures proposed in Part 2 or not and whether to take any additional actions that may not have been proposed by the Data Protection Leader in Part 2	
Date and time Parts 1-3 sent to Data Protection Leader and/or any other public official tasked with assisting with the response to the incident/breach	

Part 4: Personal Data Breach Notifications & Other Actions Taken ***This part should only be completed by the Data Protection Leader/other responsible person if the Chief Officer/Head of Department declared the incident a personal data breach in Part 4.*** All personal data breaches must be (a) assessed to determine if it is likely to prejudice the rights and freedoms of the affected data subjects; and (b) reported in accordance with the Data Protection Act. This section may be updated to confirm actions as they are proposed, in progress and completed. You may wish to use bulleted or numbered lists in these cells and note the date each measure is completed. The breach file will be formally closed only after all proposed measures, that have been accepted by the relevant person with appropriate authority, have been taken and all notifications have been completed.	
Likely consequences of the breach for data subjects (e.g. e.g. nuisance, emotional harm, reputational damage, physical harm, financial harm)	
Measures that have been recommended for data subject(s) to mitigate possible adverse effects	
Measures *already taken/ completed* by the Data Controller to address the breach and/or mitigate its adverse effects	
Measures *in progress* by the Data Controller to address the breach and/or mitigate its adverse effects	
Further measures *proposed* by the Data Controller to address the breach and/or mitigate its adverse effects	
Date, time and method Ombudsman notified	
Date(s), time(s) and method(s) affected data subjects notified	
Date and time personal data breach file closed, with no further action required	
Name, title and department of Data Protection Leader closing the file	

PERSONAL DATA BREACH NOTIFICATION TEMPLATE

Dear [Name of Data Subject],

The Ministry of Education (the Ministry) respects your privacy and takes care in processing your personal data. Pursuant to section 16 of the Data Protection Act (2021 Revision), we are notifying you that your personal data were subject to a personal data breach.

The breach occurred [*State when the breach first occurred or the length of time that it occurred (if this is known) and when it was discovered (if this is not the same time). Describe the nature of the breach but do not disclose information that would constitute a security risk or cause harm to the Ministry, to the data subject, or to a third party. What happened? Was this a breach of confidentiality, integrity or availability? How many data subjects were impacted? What type of personal data were involved?*]. The consequences of the breach are [*Describe the consequences of the breach, which should clearly relate to the nature of the breach. Consider the likely impact of the breach, with a particular focus on potential harm or risk to the rights and freedoms of the data subject.]*

We have taken or will take the following measures to address the breach:

- [*Describe the measures taken or to be taken by the Ministry to address the breach*]
- [*Measures taken by the Ministry will include specific mitigating actions to contain the breach (e.g. taking a service offline if it is incorrectly configured and disclosing personal data to the wrong users) and reduce the risk of harm from this specific breach (e.g. forcing a password reset for all users if passwords were compromised) as well as more general actions that have been taken or will be taken to reduce the risk of a similar breach (e.g. training staff)*]; and
- [*As an example of a specific mitigating action, where personal data were emailed to the wrong person, it is expected that the Ministry will contact the person(s) who should not have received the personal data, ask them to not view the data, to immediately and permanently delete the email and any attachments, and to confirm back in writing when this has been done*].

We recommend that you also [*Describe any measures that you, as the Ministry, recommend the data subject take to mitigate the impact of the breach, e.g. to reset passwords if they used a breached password for another purpose, to be even more attentive to possible phishing emails or other spam if their email address was disclosed without authorisation or subject to a hacking exfiltration, or to not "reply-all" to provide information requested in an email that was not sent using the "Bcc" function.*].

On behalf of the Ministry, I apologise that our security measures did not prevent this breach [*if appropriate, also state "and for any harm this may cause you"*]. We are committed to continually improving our privacy practices and have also notified the Ombudsman of this breach.

If you have any questions about this personal data breach, please let me know.

Sincerely,

[Name]
Data Protection Leader for the Ministry of Education
[Contact Details]