RCIPS

Office of the Commissioner of Police (OCP)

Data Protection Policy

Data Protection Policy

Version 1.0 – 2022, April

ITEM	DETAILS
Security Classification	NOT PROECTIVELY MARKED
Disclosable Under FOI	**Yes**
Document Title	**DATA PROTECTION POLICY**
Strategic/Portfolio Lead	Commissioner of Police
Owner	Commissioner of Police
Author	Data Protection Manager
Approval Date	12th April 2022
Implementation Date	12th April 2022
Date of current publication or review	12th April 2022
Previous Review(s)	Original
Filing	Strategic Transformation & Project Management Office
This document is a controlled document that supersedes all previous versions. Please discard any previous copies of this document dated prior to the version and publication date noted above this page.	

Table of Contents

1. EXECUTIVE SUMMARY

This Data Protection Policy ("this Policy") establishes how The Office of the Commissioner of Police (OCP) protects Personal Data based on the Cayman Islands Data Protection Act (2021 Revision) ("DPA") the Data Protection Regulations, 2018 ("Regulations") and in line with the Cayman Islands Government Privacy Policy.

This Policy ensures OCP employees, other Public Officials and suppliers who have access to Personal Data processed by the OCP understand the rules governing the use of Personal Data.

2. INTRODUCTION

2.1 Background

When delivering public policies, programmes and services, the OCP 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 OCP will be provided directly by the individual (i.e. the Data Subject). However, the OCP may also receive Personal Data indirectly (e.g. when conducting a background check or from another Public Authority in the course of their duties).

The OCP must only use Personal Data to deliver public policies, programmes and services, including under enabling legislation, and 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.

2.2 Purpose and Objectives

Implementing and complying with this Policy will enable the OCP'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:

a. facilitate statutory and regulatory compliance by the OCP in accordance with applicable legislation;
b. promote consistency in practices and procedures; and
c. 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 OCP, which includes the Royal Cayman Islands Police Service (RCIPS) and the Cayman Islands Coast Guard (CICG) all Data Processors engaged by the OCP, 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 OCP is the Data Controller, a Joint Data Controller, or a Data Processor. This Policy must be used in combination with other CIG policies and procedures and those relevant to the OCP, including Privacy Notices, MOUs and all other legislation relevant to the OCP.

3. ENABLING LEGISLATION AND KEY POLICIES

The DPA along with the Regulations serve as the key enabling legislation for this Policy. As a Public Authority, the OCP 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 (2019 Revision) (as amended); and other legislation.

The following enactments are also enabling legislation for this Policy:

- Criminal Procedure Code (2021 Revision)
- Criminal Records (Spent Convictions) Act (2018 Revision)
- Penal Code (2019 Revision)
- Police Act (2021 Revision)

4. DEFINITIONS AND ABBREVIATIONS

The Office of the Commissioner of Police which comprises the Royal Cayman Island Police Service and the Cayman Islands Coastguard will be known throughout this policy as the OCP.

This Policy must be read with the **CIG Privacy Policy**. Key data protection terms and abbreviations, including those which are capitalised throughout this Policy, are defined in the DPA and in section 4 of the **CIG Privacy Policy**.

5. ROLES AND RESPONSIBILITIES

Data protection roles and responsibilities across the CIG are outlined in section 6 of the **CIG Privacy Policy**. See also **CIG Privacy Policy Appendix C: RASCI Matrix** for a complete table that defines the persons who are Responsible, Accountable, Supporting, Consulted and Informed ("RASCI") in relation to specific data protection activities.

The OCP is supported by an internal IT Unit which supports the Computer Services Department.

6. POLICY REQUIREMENTS

6.1 Data Protection Principles

6.1.1 The OCP is considered to be a Data Controller – having determined the purposes, conditions and manner in which Personal Data are Processed – and is responsible for compliance with the DPA, including the Data Protection Principles.

6.1.2 The Data Protection Principles define the OCP's responsibilities in protecting Personal Data. All OCP 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 OCP are obligated to handle Personal Data in alignment with these principles.

6.1.3 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:

a. Processed lawfully, fairly and in a transparent manner in relation to the Data Subject;
b. Collected for specified, explicit and legitimate purposes and not further Processed in a manner that is incompatible with those purposes;
c. Adequate, relevant, and limited to what is necessary in relation to the purposes for which they are collected or further Processed;
d. 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;
e. Kept for only as long as it is needed and subsequently destroyed; The OCP will ensure the purposes of Processing clearly include the legal obligation. The OCP has 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;
f. Processed in accordance with the rights of Data Subjects, including under the DPA;
g. 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
h. 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.

6.2 Legal Bases / Conditions of Processing

6.2.1 It is the OCP's responsibility to understand the different legal bases for Processing Personal Data and ensure the OCP has 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 also applies to disclosure of and providing access to Personal Data between the OCP and other Data Controllers.

6.2.2 The OCP shall ensure that one or more legal bases will be satisfied whenever Personal Data are Processed. The OCP shall identify and document 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.

6.2.3 The OCP 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.

6.2.4 The OCP shall document and review the legal bases of its Personal Data and Sensitive Personal Data Processing activities, including any information recorded in RoPAs (if applicable), at appropriate intervals to ensure compliance with the DPA and promote accountability.

6.3 Purpose Limitation and Data Minimisation

6.3.1 The OCP shall clearly identify and document the purposes for Processing Personal Data.

6.3.2 The OCP shall ensure that the purposes for Processing Personal Data are included in the OCP's Privacy Notices. See **Privacy Notices** (section 6.6) for more details.

6.3.3 The OCP shall ensure that when new purposes for Processing Personal Data are identified, the OCP is satisfied that one of the following applies:

a. The new purpose is not incompatible with the original purpose; or
b. The Processing is exempt from the second Data Protection Principle (purpose limitation) pursuant to a specific provision in Part 4 of the DPA; or
c. The OCP 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, including the Data Protection Principles.

6.3.4 The OCP shall ensure the Personal Data collected 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.

6.3.5 The OCP shall ensure that when Personal Data are no longer needed for specified purposes, they are destroyed, secured, archived or anonymised in accordance with the OCP's data retention guidelines. See **Data Retention and Disposal** (section 6.10) for more details.

6.3.6 The OCP shall ensure that only the minimum amount of Personal Data needed to fulfil the purpose or purposes are requested.

6.3.7 The OCP shall review its data Processing periodically to check that the Personal Data the OCP holds are still relevant and adequate for the purposes of Processing.

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

6.4.1 The OCP shall comprehensively inventory and map the Processing of Personal Data by the OCP and keep these records up-to-date.

6.4.2 A full records survey has been carried out across the OCP which comprises all records stored and used within units across the organisation.

6.4.3 Further work will take place to develop the records survey in line with the implementation of a full ROPA.

6.4.4 The OCP shall create and maintain a RoPA and keep an overview of all Processing activities the OCP operates.

6.4.5 The OCP shall ensure the RoPA includes the following as a Data Controller or a Joint Data Controller:

a. The OCP's name and contact details, and, where applicable, the name of the Joint Data Controller, their representative and the Data Protection Manager;
b. The purposes of the Processing of Personal Data;
c. A description of the categories of Data Subjects and categories of Personal Data;
d. The categories of Recipients of Personal Data;
e. Details of transfers to any countries or territories outside of the Cayman Islands, including a record of the transfer mechanism and safeguards in place;
f. Retention schedules, which may reference the relevant disposal schedule; and
g. A description of the technical and organisational security measures in place.

6.4.6 The OCP shall ensure the RoPA includes the following if acting as a Data Processor:

a. The OCP's name and contact details and the name and representative of each Data Controller on behalf of which the Data Processor is acting (and, where applicable, the Data Controller's DPO or Data Protection Leader);
b. The categories of Processing carried out on behalf of each Data Controller;
c. Details of transfers to countries or territories outside of the Cayman Islands, including a record of the transfer mechanism safeguards in place; and
d. A description of the technical and organisational security measures in place.

6.4.7 The OCP shall create and maintain an internal record of all Processing activities carried out by any Data Processors on behalf of the OCP.

6.4.8 The OCP shall implement processes to review and update data inventories, data maps and the RoPA at appropriate intervals, at least once every two years and as soon as practicable when there are changes to processes, purposes for Processing Personal Data, new Recipients of Personal Data, new technologies, and/or legislative changes.

6.5 Consent

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 the OCP, 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:

6.5.1 To ensure any Consent that may be collected is valid:

a. The Data Subject must give Consent prior to Processing;
b. 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 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;
c. The Consent must be freely given, specific, informed and unambiguous;

d. What the Data Subject has given Consent to (purpose or purposes) must be clearly documented;
e. When and how the Data Subject has given Consent must be able to be proven;
f. The Data Subject must be able to withdraw the Consent at any time; and
g. The Processing of Personal Data on the basis of Consent must be stopped if Consent is withdrawn.

6.5.2 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. The granting of Consent should always be documented in a way that will allow the OCP to prove the Consent was given.

6.5.3 The OCP shall implement appropriate measures where Consent from Children or other vulnerable Data Subjects is required, including verifiable Consent of the Data Subject's parent(s)/guardian(s) or age-verification and/or competence-verification measures.

6.5.4 The OCP shall implement processes to review and refresh Consent at appropriate intervals, at least once every two years.

6.6 Privacy Notices

Under the DPA, the OCP is required to provide information to Data Subjects on the purposes for which the OCP Processes their Personal Data. The OCP may also be required to provide additional detailed, specific information about OCP's Processing activities, including in response to a SAR. The OCP shall 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.

6.6.1 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.

6.6.2 Privacy Notices must contain, at minimum, the identity of the OCP as a Data Controller 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.

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

6.6.4 The OCP shall update its Privacy Notices and communicate the changes to Data Subjects before starting any new Processing if the OCP plans to use Personal Data for a new purpose that is incompatible with the original purpose.

6.6.5 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, applicable retention periods, security measures, etc.

6.6.6 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.

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

6.6.8 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 OCP.

6.7 Individual Rights

The OCP shall Process Personal Data in accordance with Data Subjects' rights. This means that the OCP shall ensure there are measures implemented that allow individuals to exercise their rights under relevant legislation, including the DPA. Furthermore, the OCP shall respect and honour these rights in compliance with applicable legislation.

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

6.7.1 **The right to be informed**: The right to obtain information regarding why and how their Personal Data are Processed by the OCP, with limited exemptions.

a. The Data Subject shall receive information directly or be referred to the Privacy Notice published by the OCP if the Privacy Notice provides all of the required information.

6.7.2 **The right of access**: The right to request access to the Personal Data the OCP maintains on the Data Subject and to supplementary information about the Processing, with limited exemptions.

a. All OCP employees are required to be trained on how to recognise a SAR and understand when a SAR applies.

b. All OCP employees are required to immediately report a SAR to the Data Protection Manager. See **Subject Access Requests (SARs)** (section 6.8) for more details.

6.7.3 **Rights in relation to inaccurate data**: The right for Inaccurate Personal Data Processed by the OCP 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 a Public Authority to rectify, block, erase or destroy Inaccurate Personal Data.

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

b. All OCP employees are required to immediately report complaints regarding Inaccurate Personal Data to the Data Protection Manager.
c. The OCP 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.
d. The OCP shall ensure there are procedures in place to inform Data Subjects if and when the OCP rectifies, blocks, erases or destroys any Inaccurate Personal Data following a complaint or request from the Data Subject or an order from the Ombudsman.
e. The OCP shall ensure that when 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 OCP responds to the Data Subject in a timely manner and explains the reasons for closing the complaint or denying the request.
f. The OCP shall ensure Process Owners maintain an up-to-date log of complaints in relation to Inaccurate Personal Data and requests to rectify, block, erase or destroy Personal Data, where those complaints and requests relate to processes within their control.
g. The OCP shall ensure the Data Protection Manager maintains an up-to-date log of orders from the Ombudsman to rectify, block, erase or destroy Inaccurate Personal Data and action taken by the OCP to comply with such orders; and
h. The OCP shall ensure that appropriate systems are in place to rectify Inaccurate Personal Data or ensure Inaccurate Personal Data can be blocked, erased or destroyed if rectification is not possible or appropriate in the circumstances. See **Data Accuracy** (section 6.9) for more details.

6.7.4 **The right to restrict or stop Processing**: The right to stop or restrict the OCP's use of their Personal Data, under certain conditions.

a. All OCP employees are required to be trained on how to recognise a notice from a Data Subject to stop or restrict Processing of Personal Data.
b. All OCP employees are required to immediately report notices to stop or restrict Processing of Personal Data to the Data Protection Manager.
c. The OCP shall ensure there are processes in place to respond without undue delay to a notice from a Data Subject who requires that the OCP stop or restrict Processing of their Personal Data in whole, in relation to certain purposes, in certain matters.
d. The OCP shall ensure there are procedures in place to inform Data Subjects if and when the OCP stops or restricts Processing of the Data Subject's Personal Data in response to a notice from the Data Subject.
e. The OCP shall ensure that if a notice to stop or restrict Processing of Personal Data is lawfully denied, the OCP responds 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.

f. The OCP shall have processes in place to identify and document situations where a Data Subject has applied to the Ombudsman following the failure of the OCP to comply with a notice or request to stop or restrict Processing.
g. The OCP shall ensure Process Owners maintain an up-to-date log of notices to stop or restrict Processing of Personal Data, where the notices relate to processes within their control.
h. The OCP shall ensure there are processes in place to stop or restrict Processing of Personal Data on its systems without undue delay; and
i. The OCP shall ensure there are processes in place to indicate that Processing of Personal Data is restricted on its systems.

6.7.5 **The right to stop direct marketing:** The right to cease the use of Personal Data for direct marketing purposes by the OCP.

At this time, the OCP does not conduct any direct marketing. The OCP 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. 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".

6.7.6 **Rights in relation to automated decision-making:** The right to receive information on and object to the Processing of Personal Data using automated means where a decision is made by the OCP that significantly affects the Data Subject, under certain conditions. At this time, the OCP does not make any decisions based on the automated Processing of Personal Data. The OCP recognises 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.

6.7.7 **The right to complain:** Data Subjects have the right to make a complaint to the Ombudsman about any perceived violation of the DPA by the OCP.

a. The OCP shall ensure that there are processes in place to allow complaints to be received and resolved by the OCP before escalation to the Ombudsman. The Data Protection will lead on the response to a complaint from a Data Subject
b. The OCP shall ensure that an up-to-date log of complaints about any perceived violation of the DPA is maintained by the Data Protection Leader.

6.7.8 **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 OCP.

6.8 Subject Access Requests (SARs)

6.8.1 As part of the day-to-day operations of the OCP, an employee of the OCP may receive SARs 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 OCP.

6.8.2 The OCP shall ensure all employees know what information, including Personal Data, can be provided to Data Subjects in the normal course of business or under other policies and procedures and when employees must refer a Data Subject or their representative to the Information Manager or Data Protection Manager in accordance with this Policy, including for assistance in formulating a SAR.

6.8.3 All SARs received by the OCP shall be forwarded immediately to the Information Manager or Data Protection Manager.

6.8.4 The Information Manager or Data Protection Manager will be responsible for handling SARs in accordance with the DPA. A SAR may also be treated as a Freedom of Information request if appropriate. The OCP shall make reasonable efforts to process SARs 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; and

6.8.5 The OCP shall ensure that an up-to-date log of SARs is maintained by the Information Manager or Data Protection Manager.

6.9 Data Accuracy

6.9.1 Through reasonable and appropriate measures (i.e. processes and/or tools), the OCP shall ensure that Personal Data Processed by the OCP, 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.

6.9.2 The OCP shall carefully consider any challenges to the accuracy of Personal Data and implement processes 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. See also **Rights in relation to inaccurate data** (section 6.7.3); and

6.9.3 If Inaccurate Personal Data have been shared with Third Parties by the OCP 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 Data Retention and Disposal

6.10.1 The OCP 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.

6.10.2 The OCP's Data Retention Policy and relevant disposal schedules set out minimum retention periods and the OCP will adhere to that policy and those schedules.

6.10.3 The OCP 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.

6.10.4 When the OCP securely deletes and destroys Personal Data that are no longer required, the OCP shall make every endeavour 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) Personal Data in order to comply with applicable laws or court orders.

6.10.5 The OCP shall align retention policies and disposal schedules with the DPA, **CIG Privacy Policy** and other relevant policies and frameworks.

6.10.6 The OCP 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.

6.10.7 See the OCP **Data Retention Policy** for more details.

6.11 Data Protection Impact Assessments (DPIAs)

6.11.1 The OCP 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.

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

6.11.3 As part of the risk analysis, the OCP shall carry out an assessment of the impact of the planned Processing on the protection of Personal Data using established DPIA procedures; and

6.11.4 Where the OCP is drawing up administrative measures or rules relating to the protection of Data Subjects' rights and freedoms with regard to Personal Data Processing, the OCP 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.

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

6.12.1 Prior to sharing Personal Data with a Joint Data Controller, sharing Personal Data with a Data Processor, or disclosing Personal Data to a Third Party, the OCP shall ensure that the proposed Processing 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 Processing. See also **Legal Bases / Conditions of Processing** (section 6.2).

6.12.2 The OCP shall ensure that Data Processors comply with the Data Protection Principles when Processing Personal Data on behalf of the OCP as the Data Controller.

6.12.3 The OCP shall ensure all parties have sufficient clarity in relation to data protection roles, responsibilities and requirements, including through the establishment of appropriate

written contractual measures via an MOU or Data Processing Agreement, when any of the following situations occur:

a. The OCP, as a Data Controller, uses a Data Processor to Process Personal Data;
b. The OCP, acting as a Data Processor, engages another Data Processor (i.e. Sub-Processor);
c. The OCP and one or more other Data Controllers are identified as Joint Data Controllers; and/or
d. The OCP as a Data Controller regularly discloses Personal Data to a Third Party, including another Public Authority.

6.12.4 Where the OCP engages a Data Processor, the terms and conditions of the sharing of Personal Data shall be documented in an MOU (between Public Authorities) or in a Data Processing Agreement (between a Public Authority and a non-CIG Data Processor).

6.12.5 The OCP shall ensure that all Data Processors providing services to the OCP are contractually required to follow the policies set forth herein, or substantially equivalent standards, and to protect Personal Data in accordance with all relevant laws, regulations and rules, and subject to any appropriate security measures
and directions from the OCP. These requirements should also apply to any subcontractors that may be engaged by the Data Processor; and

6.12.6 Prior to disclosing Personal Data to a Third Party, the OCP shall 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.

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 OCP shall refrain from transferring Personal Data to countries or territories that do not have adequate protections for Personal Data. This means that the OCP 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. See **CIG Privacy Policy Appendix D: International Transfers** for more details.

6.13.2 The OCP 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 before Personal Data are transferred internationally to that Data Processor, and that such contracts contain appropriate Data Protection clauses.

6.13.3 The OCP shall ensure that where Personal Data would be transferred to a Recipient located outside the Cayman Islands, measures are in place to ensure that appropriate international data transfer mechanisms are designed, adopted and implemented prior to the transfer to

ensure that Personal Data that are or may be transferred internationally are adequately protected; and

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

6.14 Security

6.14.1 The OCP 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.

6.14.2 The OCP shall adopt the **CIG Information Security Policy**.

6.14.3 The OCP uses a range of physical, technical and organisational measures to safeguard Personal Data. These measures include but are not limited to:

a. Developing and maintaining written plans to identify, prevent, detect, respond to, and recover from security threats, events and incidents;
b. Developing robust authentication procedures for accessing all systems that store Personal Data;
c. Administrative and technical controls to restrict access to Personal Data on a "need to know" basis;
d. 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, including through actions such as patching, licence renewals/expiry monitoring, system health checks and account/user access management;
e. Requiring Data Processors who Process Personal Data on behalf of the OCP to maintain appropriate security measures, including through MOUs or Data Processing Agreements;
f. Maintaining appropriate records of access to and Processing of Personal Data;
g. Ensuring employees are trained on security policies and measures that have been implemented;
h. 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;
i. 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;
j. Utilising appropriate and secure methods to destroy Personal Data as legally required; and

k. Taking all other reasonable measures as required from time to time by legislation, rules and policies; and
l. Physical security of premises.

6.15 Incident Reporting and Response

6.15.1 The OCP shall ensure that the suspected theft, loss or unavailability of Personal Data, other unauthorised Processing of Personal Data, or damage to Personal Data is immediately investigated.

6.15.2 The OCP 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.

6.15.3 The OCP shall adopt the **CIG Information Security Incident Management Policy & Procedure** and shall also develop and maintain appropriate supplementary incident response protocols tailored to the OCP and the different types of incidents / threats in order to ensure any Personal Data Breach can be efficiently responded to and reported as required by law.

6.15.4 The OCP shall, at minimum, perform a table top walkthrough of its incident response protocols at regular intervals to determine the effectiveness of those protocols and identify areas for improvement; and

6.15.5 The OCP employees shall immediately report any suspected security incidents involving Personal Data to their manager or to the Data Protection Leader.

6.16 Personal Data Breach Notification

6.16.1 The Data Protection Leader shall be notified of any suspected or actual Personal Data Breach in accordance with the OCP security incident response protocols or in accordance with the MOU / Data Processing Agreement where the OCP has engaged a Data Processor, is serving as a Data Processor, or is a Joint Data Controller with another Public Authority.

6.16.2 In the event of a security incident involving Personal Data, the Data Protection Leader, shall investigate the incident to determine whether a Personal Data Breach has occurred. All Public Officials and Data Processors shall assist with an investigation if required.

6.16.3 Only the Chief Officer shall be authorised to determine that a Personal Data Breach has occurred and may be advised on this matter by other persons as appropriate.

6.16.4 The OCP shall assess each Personal Data Breach to determine whether it is likely to prejudice the rights and freedoms of the affected Data Subjects.

6.16.5 The Data Protection Leader shall, under the direction of the Commissioner of Police and Deputy Commissioner of Police, 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 shall describe, at minimum:

a. the nature of the breach;
b. the consequences of the breach;
c. measures taken or proposed to be taken by the OCP to address the breach; and
d. measures recommended by the OCP to the Data Subject to mitigate the possible adverse effects of the breach.

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

a. the nature of the breach;
b. likely consequences of the breach for Data Subjects;
c. categories of Data Subjects concerned;
d. types and amount of Personal Data involved;
e. the cause of the incident (if known);
f. how the breach was identified;
g. the date and time the breach occurred (if known);
h. the location and duration of the incident;
i. the date and time the breach was identified;
j. if the breach occurred at a Data Processor, the identity of the Data Processor;
k. remedial actions proposed to be taken to address the breach;
l. remedial actions taken to address the breach;
m. when the breach was reported to the Ombudsman and to affected Data Subjects; and
n. when the case was closed.

6.17 Training and Awareness

6.17.1 The OCP shall ensure that all OCP 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.

6.17.2 All employees of the OCP 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.

6.17.3 The OCP 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.

6.17.4 All Recipients of Personal Data Processed by the OCP shall be made aware of both their individual responsibilities and of the OCP's responsibilities under the DPA and under this Policy; and

6.17.5 The OCP shall ensure that all its employees receive and attend training to identify SARs and other requests or notices where Data Subjects are seeking to exercise other Data Subject Rights, and how to respond or forward the request or notice to the Information Manager or Data Protection Manager. See also **Individual Rights** (section 6.7).

6.18 Acting as a Data Processor

The OCP will be considered a Data Processor when 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 OCP acting as a Data Processor are:

6.18.1 Ensuring that an MOU or Data Processing Agreement is in place with the Data Controller(s);
6.18.2 Ensuring that all activities and tasks of the OCP are carried as agreed in the MOU or Data Processing Agreement;
6.18.3 Maintaining a RoPA as required, including as per the MOU or Data Processing Agreement. See also **Data Inventory, Data Mapping and Record of Processing Activities (RoPA)** (section 6.4.5);
6.18.4 Implementing appropriate security measures to protect the Personal Data Processed by the OCP on behalf of the Data Controller;
6.18.5 Informing the Data Controller in the event of a Personal Data Breach within the stipulated timeframe outlined in the MOU or Data Processing Agreement; and
6.18.6 If responsible as per the MOU or Data Processing Agreement, informing the Ombudsman of Personal Data Breaches within the stipulated timeframe(s), subject to any exemptions that may apply.

6.19 Exemptions

An exemption applies where some or all requirements or rights of the DPA are changed in relation to specific Personal Data Processing. Some exemptions are partial (i.e. allowing the Data Controller or Data Processor to not follow certain provisions, provided certain circumstances exist and/or other provisions are followed). They are generally specific to particular provisions or requirements of the DPA and set out in Part 4 of the DPA (Exemptions). All other provisions of the DPA, outside of the specified exemption, continue to apply.

The following exemptions from aspects of the DPA are most likely to be relevant to the Personal Data Processed by the OCP and must be considered in the implementation of this Policy:

Section 19 – Crime, government fees and duties

Personal data processed for the purposes of the prevention, detection or investigation of crime, the apprehension or prosecution of persons who are suspected to have committed an offence anywhere or the assessment or collection of any fees or duty, or any imposition of a similar nature are exempt from the first data protection principle (except to the extent to which it requires compliance with the conditions in Schedules 2 and 3), the non-disclosure provisions and section 8, to the extent to which the application of those provisions would be likely to prejudice any of the matters referred to in paragraphs (a) to (c).

7. DATA PROTECTION LEADER

The OCP 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**.

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, please contact the Data Protection Leader.

Name: Darren Rigg

Phone Number: 649 2938

Email Address: Darren.Rigg@rcips.ky

Address: Royal Bank of Canada Building, 4th Floor, 24 Shedden Road, George Town, Grand Cayman, Cayman Islands

8. POLICY MONITORING AND COMPLIANCE

Measuring compliance with this Policy is part of the responsibilities of the Data Protection Manager.

Violation of this Policy may result in disciplinary action up to and including termination of employment.

Legal sanctions may also be pursued, if appropriate and as defined by the DPA or other relevant legislation.

9. POLICY EVALUATION AND CHANGE

Any employee of the OCP 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 Manager in consultation with the senior management team for its completeness, adequacy, and alignment to the functions and priorities of the OCP 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 Commissioner of Police.