

# **Employee Privacy Notice**

## **1. Scope**

The Office of the Commissioner of Police, (OCP), respects your privacy as an employee and takes care in protecting your personal data. As a Data Controller, we comply with the Cayman Islands Data Protection Act (2021 Revision) (the “DPA”).

This employee privacy notice (“Employee Privacy Notice”) demonstrates our commitment to ensuring your personal data will be handled responsibly and applies to the OCP. It sets out how we collect, record, use, disclose, store, retain and dispose of your personal data during and after your period of employment with us.

This Employee Privacy Notice does not cover:

- a. the recruitment and selection process that was undertaken prior to your employment with us (if you applied for your role after the launch of the CIG e-recruitment platform, the CAREERS.GOV.KY privacy notice is available at <https://careers.gov.ky/application/custom/English/privacy-statement.html>);
- b. public services and programmes that we offer to individuals who are not our employees;
- c. public officials who are not employees of the OCP, e.g. if you are a contractor, a Minister, a Parliamentary Secretary, or a member of a board, committee, tribunal, council, commission, etc.

Our external privacy notices are available at <https://www.rcips.ky/privacy-policy>.

Other Ministries, Portfolios, Offices, Departments, Sections, Units, Statutory Authorities, Statutory Bodies and Government Companies may also process your personal data as an employee of the Cayman Islands Government. This Employee Privacy Notice does not include information on behalf of these separate Data Controllers.

This Employee Privacy Notice does not form part of your Employment Agreement and may be updated at any time.

## **2. What Personal Data We Collect**

The OCP collected personal data about you through the application and recruitment process, either directly from you or from third parties such as a referee.

The OCP will also collect and record additional personal data about you in the course of your work-related activities as you deliver on Government priorities – for example, from your manager, through feedback provided by your colleagues across the CIG, and the people we serve. We may also collect your personal data in the course of our administrative functions, for example staff administration, procurement, property management, advertising and media.

In some cases, your personal data will be collected indirectly through various monitoring systems and devices. If these types of personal data are collected for security purposes, they are not generally accessed on a routine basis.

Personal data recorded or collected by the OCP is limited to what is necessary for our processing activities. In this Employee Privacy Notice, “personal data” means any data relating to you as a living individual where you are identified or identifiable. “Personal data” includes “sensitive personal data” as defined in the DPA.

The OCP may record or collect the following information about you as an employee:

- a. name, date of birth, photograph(s), address and contact details;
- b. personal data contained within your government-issued identification document(s);
- c. citizenship/nationality and immigration status in the Cayman Islands;
- d. details of your emergency contact(s) and dependent(s) and their relationship to you;

- e. job/role description, working conditions, salary/wages and benefits;
- f. time and attendance records, which may include information relating to physical and mental health conditions, injury or disability, your family relationships and other relevant information, if required;
- g. details of any official travel you may undertake during your employment;
- h. work objectives and job performance, including complaints and disciplinary action;
- i. training, qualifications, and learning and development activities;
- j. any personal data that would be relevant to a workplace investigation, including investigations arising from complaints, grievances, and alleged or potential breaches of the Public Servant's Code of Conduct;
- k. criminal convictions and information about your commission, or alleged commission, of a criminal offence and any proceedings related to that office, if appropriate due to the nature of your job;
- l. Personal data collected via CCTV at the OCP premises, including images via camera located at office accommodation across the OCP estate; and
- m. any information you choose to provide when interacting with the OCP during your time as an employee, including on social media platforms and in surveys and other feedback mechanisms.

### **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 OCP operates a personnel policy that complies with the principle of being a good employer. We aspire to be an employer who cares and to adhere to the highest ethical, moral and professional standards at all times. As your employer, the OCP may use your personal data for the following purposes:

- a. To perform our obligations under the Employment Agreement entered into with you, and to perform key employment management activities (e.g. pay your salary, facilitate benefits management services, allocate and manage duties and responsibilities, business continuity planning and dealing with incidents). Your personal data will or may be processed as a condition for your continued employment with the OCP and may include medical exams, drug tests or fitness tests during the employment period;
- b. To ascertain your fitness for work and to manage absences, including absence related to sickness;
- c. To gather evidence and take other steps relating to any complaints, grievances, disciplinary matters and other investigations as well as any associated hearings or other types of resolution processes;
- d. To comply with our legal obligations, including to make and maintain full and accurate public records, and uphold the Public Service Values which govern the management and operation of the Civil Service;
- e. Succession planning and effective management of current and future vacancies and workforce needs;
- f. To manage risk, prevent fraud and corruption, and protect public funds and the integrity of the Civil Service, including facilitating or cooperating with internal and external reviews, audits and investigations;
- g. To implement information security controls and investigate security events and incidents;
- h. To seek legal advice and exercise or defend legal rights;
- i. To respond to your inquiries and requests;
- j. Reporting and statistical purposes, including analysing data and using it to make informed decisions;

- k. Consultation and employee engagement, including administering surveys or seeking your feedback in other ways, communicating with you, and planning and hosting employee social activities and events;
- l. External communications and public relations, including celebrating our successes on social media and other channels, which may reference employees and/or include your photograph and other information; and
- m. If it is necessary to disclose your personal data to a third party for legitimate interests pursued by the OCP or by the third party to whom your personal data would be disclosed, including under the Freedom of Information Act (2021 Revision). If we receive a Freedom of Information (FOI) request for records that include your personal data, we will always consult with you in writing if we are considering disclosing any personal data other than your name, official contact details, and the general terms upon and subject to which you occupy your post in the public service – which do not constitute “personal information” as defined under the Freedom of Information (General) Regulations (2021 Revision).

#### 4. How We Share Your Personal Data

The OCP may share your personal data as required, including under applicable legislation, with recipients that include our Data Processors and third parties. We will only share your personal data as permitted by the DPA and in accordance with the CIG Privacy Policy.

Your personal data may be shared with the following types of recipients:

- a. **With other public authorities:** Personal data may be shared with other public authorities – here, “public authorities” means Ministries, Portfolios, Offices, Departments, Statutory Authorities, Statutory Bodies and Government Companies – as required or permitted by law and for one or more of the purposes set out in this Employee Privacy Notice. This includes but is not limited to the Portfolio of the Civil Service, Treasury Department, Computer Services Department, eGovernment Unit, Cybersecurity Unit, Office of the Auditor General, Internal Audit Service, Office of the Ombudsman, Portfolio of Legal Affairs, Public Service Pensions Board, Civil Service College the Police Service Commission and Cayman Islands National Insurance Company (CINICO).

This data sharing within the Civil Service includes disclosing your personal data to a separate Civil Service Entity if you begin working in a new or different role, whether on a temporary basis (i.e. through a secondment or redeployment) or on a permanent basis (i.e. through a transfer or after applying for and obtaining a new role) to facilitate your work in that role and to facilitate standard HR functions.

- b. **With Data Processors external to the CIG:** Personal data may be shared with persons providing services to the OCP as a Data Processor in compliance with the DPA. These service providers are only able to use personal data under our instructions and may be related to:
  - i. Webhosting;
  - ii. Information Technology;
  - iii. Records and Information Management, including storage facilities;
  - iv. Communications;
  - v. Marketing and campaigns;
  - vi. Events management; and
  - vii. Security operations and fraud prevention.
- c. **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:

- i. Seeking legal advice;
  - ii. Exercising or defending legal rights;
  - iii. Complying with internal and external audits or investigations by competent authorities;
  - iv. Complying with information security policies or requirements; and
- d. With other third parties:** Personal data may be disclosed as required or permitted by law for the purposes set out in this Employee Privacy Notice. Your name, photo and official contact details will be available to all other civil servants through the my-VISTA Employee Directory, the Hub (the CIG intranet), and (if you have a CIG email address and network account) Microsoft Outlook and other Microsoft applications.

Depending on your position with the OCP and participation in certain activities, your name, photo, contact details or other personal data – including information about your public life and official business as well as your educational background, professional qualifications and experience – may also be published on our website, in annual reports and other publications, and on our social media channels.

## 5. Our Legal Bases for Processing Your Personal Data

The OCP will rely on specific legal bases, or “conditions of processing”, under the DPA to process your personal data. These legal bases may include:

- a. A **legal obligation** to which the OCP is subject, e.g. to comply with various obligations under the Public Service Management Act (2018 Revision) and Personnel Regulations (2022 Revision), the Public Management and Finance Act (2020 Revision) and Financial Regulations (2022 Revision), the National Archive and Public Records Act (2015 Revision), the Freedom of Information Act (2021 Revision), the Complaints (Maladministration) Act (2018 Revision), the Police (Complaints by the Public) Law (2017), Standards in Public Life Act (2021 Revision)(Section 11), Cayman Islands Coast Guard Act (2021), and the Police Act (2021 Revision).
- b. To exercise our **public functions**, including under an enactment;
- c. To perform a **contract** with you, i.e. your Employment Agreement;
- d. To protect your **vital interests**;
- e. **Consent**, e.g. to administer certain surveys and polls or to participate in certain social activities; and
- f. For the purposes of **legitimate interests** pursued by the OCP or by a third party or parties to whom the personal data may be disclosed, e.g. when disclosing records containing third party personal data in response to a request submitted under the Freedom of Information Act (2021 Revision).

Where we process your sensitive personal data, as defined in the DPA, we will also meet a second legal basis. These legal bases may include:

- a. If it is necessary to exercise or perform a right, or obligation, conferred or imposed on the OCP by law – including but not limited to under the Public Service Management Act (2018 Revision) and Personnel Regulations (2022 Revision) – in connection with your **employment**;
- b. To exercise our **public functions**, including under an enactment;
- c. In relation to **legal proceedings**, including obtaining legal advice and otherwise establishing, exercising or defending legal rights; and

## 6. Security and International Transfers

The OCP has put in place appropriate technical, physical and organisational measures in order to keep your personal data secure to maintain confidentiality, integrity and availability of your personal data.

The OCP will not transfer your personal data to another country or territory unless it will be adequately protected. We may transfer your personal data outside of the Cayman Islands with the relevant safeguards based on IT services and other contractual arrangements.

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 DPA. Exceptions may include where you have provided your consent to the transfer or where the transfer is carried out on terms approved by the Ombudsman as ensuring appropriate safeguards.

## 7. How Long We Keep Your Personal Data

The OCP 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.

Records containing your personal data will be disposed of in accordance with the Cayman Islands National Archive (CINA) *Administrative Disposal Schedule #3 for Human Resource Management*, which is available to download at [cina.gov.ky/portal/pls/portal/docs/1/10422155.PDF](http://cina.gov.ky/portal/pls/portal/docs/1/10422155.PDF), and other relevant administrative or Operational Disposal Schedules. Sometimes, we may anonymise your personal data so that it is no longer associated with you in public records that are retained longer, e.g. if we aggregate certain types of employee personal data to create statistics.

## 8. Your Rights

The OCP 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 own personal data include:

- a. **The right to be informed and the right of access:** The right to request access to all personal data the OCP maintains about you as well as supplementary information about why and how we are processing your personal data, commonly known as a Subject Access Request. Certain supplementary information about our processing is contained within this Employee Privacy Notice. As a civil servant, you are also able to directly approach your manager or HR team to request any information on your personnel file. However, you have a right to file a formal Subject Access Request if you feel this is necessary.
- b. **Rights in relation to inaccurate data:** The right to request the rectification, blocking, erasure or destruction of any inaccurate personal data the OCP 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.
- c. **The right to stop or restrict processing:** The right to stop or restrict how the OCP uses your personal data in certain circumstances. The OCP is not required to comply with a notice to stop or restrict processing if it is necessary for the performance of a contract to which you are a party, i.e. your Employment Agreement, or if it is necessary to comply with any legal obligation. However, you may object to the use of your personal data in other circumstances, e.g. for promotional purposes. Certain activities will also be optional, e.g. participating in surveys or in employee social activities and events.
- d. **The right to stop direct marketing:** The right to stop the OCP from using your personal data for direct marketing purposes.

- e. **Rights in relation to automated decision making:** The right to obtain information about and object to the use of automated decision making by the OCP using your personal data.
- f. **The right to complain:** The right to complain to the Ombudsman about any perceived violation of the DPA by the OCP.
- g. **The right to seek compensation:** The right to seek compensation in the courts if you suffer damage due to a contravention of the DPA by the OCP.

You may contact the OCP, using the contact details in section 10, to make a formal Subject Access Request to access and review your personal data or to exercise any other rights provided to you under the DPA. The OCP 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.

To access information that is contained within your personnel file, you may also contact your manager or our HR team via email [RCIPSHR@rcips.ky](mailto:RCIPSHR@rcips.ky) or telephone 345-244-2900.

To learn more about your rights under the DPA, visit [www.ombudsman.ky](http://www.ombudsman.ky).

## 9. Data Protection Principles

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

- a. **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.
- b. **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.
- c. **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.
- d. **Data accuracy:** Personal data shall be accurate and, where necessary, kept up-to-date.
- e. **Storage limitation:** Personal data processed for any purpose shall not be kept for longer than is necessary for that purpose.
- f. **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.
- g. **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.
- h. **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.

## 10. How to Contact Us

The OCP has appointed a Data Protection Leader, who has operational responsibilities for data protection under the CIG Privacy Policy. If you have any questions about this Employee Privacy Notice or how your personal data are handled, or if you wish to make a complaint, please contact:

Name: Darren Rigg, Data Protection/Freedom of Information Manager

Telephone number: (W) 345-244-2900 (M) 345-649-2938

Email Address: [Darren.rigg@rcips.ky](mailto:Darren.rigg@rcips.ky)

Address: RCIPS Headquarters,  
4th Floor, RBC Building,  
24 Shedden Road,  
George Town  
P.O. Box 909  
Grand Cayman KY1-1103

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

If you would like to make a Subject Access Request, the Information Manager for the OCP, who has been appointed under the Freedom of Information Act (2021 Revision), handles these requests. Requests relating to your own personal data may be made in writing to Raymond Christian, Information Manager, email: [foi.pol@gov.ky](mailto:foi.pol@gov.ky) or [Raymond.christian@rcips.ky](mailto:Raymond.christian@rcips.ky), telephone: 345-649-2938. Depending on the scope of your request, to ensure you receive all records and information you are entitled to by law, your request may be processed under the DPA, under the Freedom of Information Act (2021 Revision), or under both enactments.

## **11. Changes to this Privacy Notice**

The OCP reserves the right to update this Employee Privacy Notice at any time and will publish a new Employee Privacy Notice when we make any updates.

From time to time, the OCP may also notify you about the processing of your personal data in other ways, including verbally and by email.

*This Privacy Notice was last updated on 4<sup>th</sup> January 2024.*