



# Official Information Management Policy

## GOVERNMENT OF THE COOK ISLANDS

Effective: May 2018

---

### Policy Statement

This Policy recognises the strategic value of official information and supports the efficient and effective management of information in an orderly and controlled manner.

The Policy provides guidance on information:

- Creation or receipt
- Classification
- Use
- Storage
- Disposal
- Preservation

### Scope

This Policy requires Public Sector Agencies to implement official information management procedures in compliance with relevant legislation and this Policy.

### Principles

The Public Service Act 2009 identifies the following values for public servants to adhere to:

Honesty	acting honestly, being truthful, and abiding by the laws of the Cook Islands
Impartiality	providing impartial advice, acting without fear or favour, and making decisions on their merits
Service	serving the people well through faithful service to the Government of the Cook Islands
Transparency	taking actions and making decisions in an open way
Accountability	being able to explain the reason for actions taken, and taking responsibility for those actions
Respect	treating the people, the Government of the Cook Islands, and colleagues with courtesy and respect
Efficiency and effectiveness	achieving good results for the Cook Islands in an economical way

---

Generally accepted principles for good record or information management are: accountability, integrity, protection, compliance, availability, retention, disposition and transparency.

### Legislation and Regulations

---

The Public Service Act 2009, Employment Relations Act 2012, Ministry of Finance and Economic Management Act 1995-96, Public Expenditure Review Committee and Audit Act 1995-96, Official Information Act 2008, Public Records Act 1984, Statistics Act 1996, Income Tax Act 1997 and other relevant legislation apply.

## Definitions

---

**Agency** means any Department, instrument, or Agent of the Crown and includes a body corporate or organisation that is wholly owned or controlled by the Crown

**Appraisal** means to assess information in terms of its value and importance

**Archives** are records over 15 years of age that are no longer used for daily administration and preserved for future reference or use. Archived records should have lasting administrative, evidential or information value

**Archives Office** refers to the National Archives Office administered by the Ministry of Cultural Development

**Current records** means records which are presently in use

**Employee** means any person who is an employee of an Agency

**Employer** means the Public Service Commissioner or Head of an Agency or their delegated authority

**Information Communications Technology (ICT)** tools enable the creation, use, dissemination, storage and archiving of information electronically

**Public records** are documentary materials of any kind or nature or description that have been created, received, or used in the course of work of agencies or in court proceedings in any court together with all exhibits and other evidence annexed

**Public Service Commissioner** means the Public Service Commissioner appointed under Article 73 of the Constitution and Section 5 of the Public Service Act 2009

**Records** any medium in or on which information is recorded. This includes: paper, electronic, magnetic tape, disc, audio tape, film, slide, or a photo

## Procedures

---

Employers are responsible for administering this Policy and ensuring all Government policies are easily accessible to employees, however the onus lies on employees to read, understand and comply with Government policies. Any person who breaches this Policy may have committed an act of misconduct and be subject to disciplinary action as specified in the Code of Conduct Policy. Employers must create an organisational culture that values information.

## Information Management

---

Information management involves creating, using, storing and archiving records and information in an orderly and controlled manner. The availability of quality, timely and reliable information for decision makers enables Agencies to be more responsive and accountable for the delivery of services. Information can be managed in electronic or paper form depending on the benefits and costs of either method.

### Electronic Records

- Is the preferred method as they take up less physical storage space and are easy to retrieve

### Paper Records

- May be used where they are necessary for evidential purposes
- They are required to reduce risk of loss or damage to e-copies

## **Employer Obligations**

---

Information is an essential component of effective management

### **Employers must:**

- Establish and oversee effective information management procedures within each Agency
- Ensure staff are trained and implement the information management procedures
- Emphasise the use of electronic means to create, use and manage information
- Ensure information integrity, relevance, quality and access is maintained
- Ensure respect for information user agreements and licensing conditions
- Protect investments in information management systems and assets
- Enable sharing of information across Agencies, while respecting security and privacy
- Ensure information disposal procedures prevent the destruction of valuable records
- Ensure archived information is protected and preserved for ease of retrieval
- Ensure employees who intentionally damage or destroy information are managed appropriately (refer to the Code of Conduct Policy)

## **Creating or Gathering Information**

---

Employees create or gather records in their daily work that become official information. Staff training on the proper creation, use, storage and archiving of records is critical to developing and maintaining an effective information management system.

Official information can be verbal, written or in other formats and should be filed or stored in a manner where the information is meaningful for decision making and is retrievable.

### **Examples of information include, but are not limited to:**

- Emails, notes, phone calls and correspondence
- Statistics, reports or information created or stored by the Agency
- Decisions made by employers and employees
- Minutes of meetings
- Personnel records: contracts, payroll, leave, performance appraisals, letters etc.

### **Agencies must have procedures to:**

- Receive and record incoming official information
- Process or despatch outgoing official information
- Maintain a filing system for records or information generated internally
- Identify information to be disseminated or distributed
- Identify information to be classified as current or inactive
- Identify and confirm information to be destroyed
- Identify information to be preserved and archived
- Protect personal information
- Protect confidential information
- Clarify how information is to be transferred to physical storage
- Clarify how e-resources are used to store and archive records

An information filing system should be maintained to control access and prevent unauthorised access and use. Employees maintaining and safeguarding information should be trained on how to use fire extinguishers and be aware of the Agency's risk management procedures.

## Classifying Information

---

Employees who create and use the records are the best appraisers of their administrative value. Records can be appraised using the following criteria:

### 1. Pre-Assessment

- What functions were the records intended to serve?
- What information is available about the processes that created the records?

### Information that can be broadly classified as operational or administrative records.

- **Operational records** are created and maintained to support the Agency's specific mandate, functions or operating activities
- **Administrative records** are maintained to support the operations of the Agency such as financial and personnel management, information technology, and building maintenance. Administrative records are common across Agencies.

### 2. Assessment

There are two general types of values records may have: primary or secondary value. Consideration of value depends on the operational or administrative functions of the Agency.

### Primary value is divided into: administrative value, financial value and legal value.

To determine whether a record has primary value, the following questions must be asked:

- Has the original purpose or function of the record been achieved?
- Is the record available from other sources?
- Should the record be destroyed or archived?

If the record is required for litigation purposes, it should be kept for up to 6 years then assessed for archiving.

### Secondary value is grouped as:

- **Evidential value** - records which contain evidence of the Agency's purpose, functions and activities. Includes: structures, legislation, functions, policies, procedures and publications
- **Informational value** - records held in other formats (microfilm) and by other Agencies, or refers to important individuals, events, subjects, groups, institutions, places, or historical developments
- **Intrinsic value** - records derived from historical or cultural organisations, with unusual formats, and original or monetary value

It is common to have duplicate records across the Public Sector due to information sharing and work or decision-making between different Agencies.

## Using Information

---

Information provides evidence or data to support decision making, policy development and effectiveness, dispute management, accountability and reporting, workforce planning and public sector reform. Information sharing across Public Sector Agencies is encouraged to enhance the performance of Agencies, except where the law requires withholding such information.

Personal information taken can only be used for the purposes for which it is taken. Individuals have a right to access their personal information and request corrections to original information that may be inaccurate. Agencies must develop processes for this.

## **Information can be used for:**

### **1. Execution of Agency functions**

- Agencies can use information to provide appropriate health care, investigate crime, collect tax revenue, approve work permits etc.

### **2. Policy development, implementation and evaluation**

- Policy analysis that requires facts and figures be well organised and managed for Managers to be aware of the current state of affairs before proposing changes
- Policy development that requires consideration of new approaches or alternative options which rely on vast research, records and information
- Policy implementation which requires cooperation between key stakeholders in sharing information and communicating activities to assess the efficiency of implementation
- Policy evaluation that is efficient and dependent on well-organised records and information

### **3. Transparency, accountability, efficiency and effectiveness**

- Meeting stakeholder requests for official information
- Assessing policy effectiveness and whether resources were used efficiently
- Demonstrating accountability for results and achieving Government's goals

### **4. People management**

- Workforce planning with statistical information on the composition of employees by Agency and associated payroll costs
- Performance improvement, training and retention strategies, and remuneration policies

### **5. Dispute management**

- Supporting resolutions of conflict between conflicting parties that require accurate information such as contracts, statistics and payroll information, that are easily retrievable

### **6. Revenue collection and resource allocation**

- Information on taxpayers must be accurate and adequate to enable collection of taxes and to improve revenue collection
- Allocation of financial resources to Agencies to deliver Government priorities requires proper records and information systems for accurate decision making

## **Storing Information**

---

### **Storage areas**

Records must be stored using appropriate filing systems or dedicated storage areas with appropriate fire protection, security and environmental controls.

Strong governance and controls over the storage of electronic information is required to mitigate the risks of unauthorised access and use. Regular back-ups and firewalls must be in place to maintain the integrity and security of data.

Physical storage areas must be protected against internal hazards such as flammable finishes or furnishings, chemicals, electrical plants, overhead pipes (other than fire suppression systems), rodent and pest invasion, mould, algae and unnecessary plumbing.

A fire protection and building maintenance programme must be in place with regular inspection for risks and prompt repairs to mitigate the risk of:

- Failure of equipment and facilities
- Fire and loss of records
- Damage from exposure to heat and smoke and extensive water damage from fire fighting
- Contamination from chemicals or sewerage
- Gradual damage from slow leaks
- Damage from rodents, pests, mould and algae

Storage areas must be readily accessible by authorised users to mitigate the risk of:

- Theft or vandalism
- Inability to control access or security to sensitive records
- Deterioration from exposure to dust, dirt, sunlight, moisture, and extreme temperature
- Deterioration from exposure to humidity and mould growth
- Deterioration or loss of records due to inappropriate storage and environmental conditions
- Damage or contamination from other material or equipment stored nearby
- Water damage due to floods or leaks from burst or blocked pipes, or below flood line storage
- Inability to access records stored on unstable media due to rapid deterioration
- Inability to access records due to equipment to read data not being available
- Inability to meet the costs of maintaining a stable environment without sealing or insulation

## **Retention**

The Limitation Act 1950 allows a civil suit to be brought up to six years after the event which gave rise to the loss or damage. For that reason, records must be kept for six years and then assessed for archiving.

Agencies must maintain record retention schedules which:

- Identify all records created or maintained by the Agency
- Note assessment decisions regarding the records
- Specify periods they are to be retained for and appropriate storage area
- Authorise disposal and disposal actions to be taken

A retention period is the length of time for which records have primary value. Agencies must have information retrieval procedures to allow access to records as required. There are two disposal options for records: (i) destruction or (ii) transfer to the National Archives Office.

## **Destroying Information**

---

There should be an approval process for the retention and disposal of records. Records with primary value should be held for periods required by law. Records with secondary value may be kept for historical or intrinsic purposes and archived. Reasonable retention periods will need to be determined by each Agency employer, guided by legislation or Government policies.

Paper records can either be shredded or incinerated. Records must not be placed in rubbish or landfill sites as this may lead to unauthorised access to confidential or sensitive information.

Documentation of destroyed records must be maintained.

## **Archives**

---

The National Archives Office stores archives over 15 years of age. Other records must be stored by Agencies in safe storage areas and must be:

- Arranged in an orderly manner
- Appropriately labelled
- Preserved for retrieval or future use
- Made available for approved research
- Continuously assessed or eventually destroyed according to an authorised procedure

Records must be kept on the use of archives, by the Agency as and when they use these services.

## **Other Provisions**

---

All records must be kept for at least seven years and are only accessible by the Employer and/or authorised staff unless lawfully accessible by other persons. After the required seven year period, the Agency may destroy or store the documentation depending on the appraised value of the information and legislation which guides the destruction or archiving of official information.

The Office of the Public Service Commissioner is responsible for reviewing and updating this Policy and associated documents from time to time.

### **Associated Documents**

- Official Information Requests Policy
- Acceptable Use of ICT Resources Policy
- Risk Management Policy
- Code of Conduct Policy

### **Other Information**

For Policy queries contact the Office of the Public Service Commissioner on phone (682) 29 421 or email: [pscinfo@cookislands.gov.ck](mailto:pscinfo@cookislands.gov.ck)