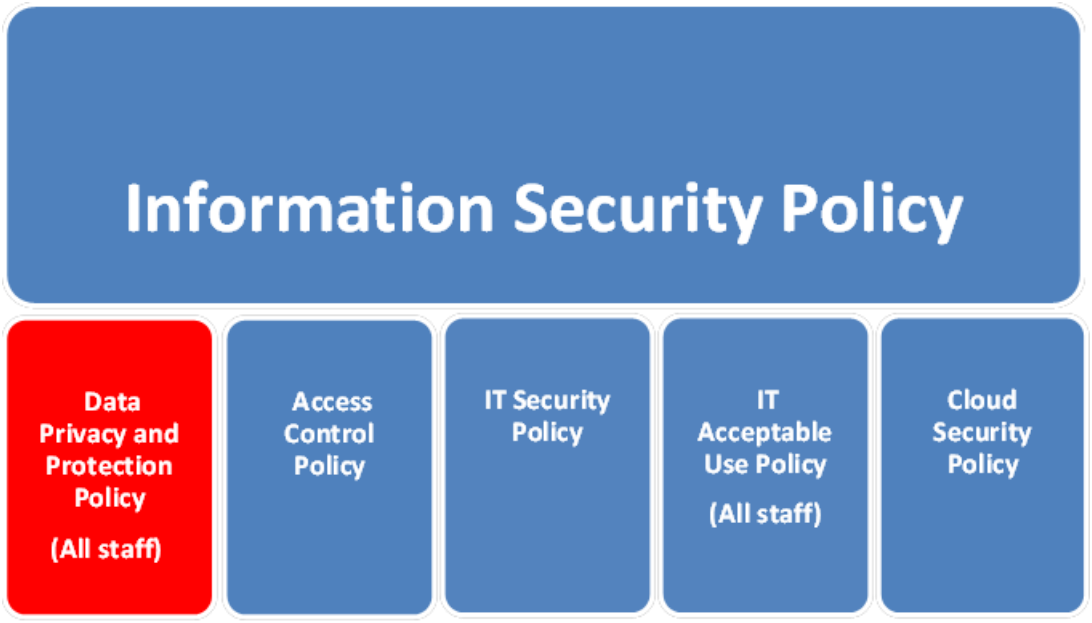
Data Privacy and Protection Policy

Table of contents



1 Purpose

This Policy is designed to articulate the way the Department of Communities and Justice (DCJ) information is to be categorised, secured, managed and used. Applying a classification to information then informs the way it needs to be secured, managed and specific restrictions regarding how it can be used.

1.1 Related documents

This document is related to the following documents:

- IT Security Policy
- IT Acceptable Use Policy
- Information Security Policy
- Access Control Policy
- Cloud Security Policy
- Data Breach Response Plan
- Mobile Devices and Wireless Connectivity Policy
- Code of Ethics and Conduct
- Enterprise Risk Management Framework and Policy
- NSW Cyber Security Policy 2020 v3.0
- NSW Government Information Classification, Labelling and Handling Guidelines
- NSW Public Service Personnel Handbook
- NSW Government Cloud Policy

2 Definitions

The table below is a list of terms, keywords and/or abbreviations used throughout this document.

Term	Definition
Approved user	A volunteer, contracted service provider, graduates, consultants, vendors engaged by DCJ and any other authorised individuals accessing DCJ systems, networks and / or information
Information asset	Any information (both physical and digital in any format, including audio and visual); Any application or ICT configuration items (CI) which stores, transmits, creates or uses information.
Information sharing	Information sharing specifically refers to a situation in which DCJ furnishes an external party with specific information as the result of a legally permissible information request. This scenario is normally authorised under a research agreement or other approved agreement. It should be noted this does not include the FOI (*Freedom of Information Act 1982*), GIPA (*Government Information (Public Access) Act 2009*) and information required to be produced by a court order. These types of requests should be responded to in compliance with legislation.
May / May not	The item is not mandatory. Recommended as best practice for consideration. No policy exception required if condition is not met.
Must	The item is mandatory. Any request for deviation from a “must” must follow the procedures for requesting exceptions.
Must not	Non-use of the item is mandatory. Any request for deviation from a “must not” must follow the procedures for requesting exceptions.
Outsourcing	Outsourcing includes any commercial arrangement where an external party stores, transfers, uses or creates DCJ information and data. This is however separate from an information sharing venture.
Should	Valid reasons to deviate from the item may exist in particular circumstances, but the full implications need to be considered before choosing a different course. No policy exception required if condition is not met.

Term	Definition
Should not	Valid reasons to implement the item may exist in particular circumstances, but the full implications need to be considered before choosing this different course. No policy exception required if condition is not met

3 Scope

Compliance with this policy is compulsory for:

- all DCJ permanent full time, part time, trainee and temporary employees and approved users.

This policy does not apply to the Judiciary who are subject to a separate policy namely the Judicial Information Security Policy.

Judicial staff including the judges' tipstaff and assistants who are DCJ employees are covered by our policies.

4 Policy statement

Information is an asset which needs to be protected appropriately to ensure its confidentiality, integrity and availability. Some of the information collected, created, transmitted and used by DCJ is personal information and is bound by privacy legislation to ensure the privacy of individuals.

As the custodians of information that is politically, commercially or personally sensitive, DCJ has a responsibility to protect information from accidental or malicious modification, unauthorised access or use, loss or disclosure.

5 Policy

5.1 Protective markings

All material in any format (e.g. hand-written, Word, JPG format) medium (online publishing platform e.g. Twitter) or resource (digital or physical materials) should be assessed to determine its classification and then labelled accordingly as per the NSW Government's Information Classification, Labelling and Handling Guidelines.

Material that may contain sensitive information needs to be labelled and managed according to the level/type of sensitivity. Sensitive material includes:

- personal information (information that identifies a person)
- health information
- information which could be subject to legal privilege
- commercial-in-confidence information
- law enforcement information

- NSW Cabinet information
- if released publicly could have an adverse effect on DCJ

Examples of sensitive information are an individual's personal details, credit information, tax file numbers, medical records, drivers licence information, criminal records, biometric information and other personal details.

It is the responsibility of all DCJ staff, third parties and consultants to ensure appropriate classification of the information they create.

OFFICIAL information is related to the DCJ's business but does not have security or sensitivity issues. This information does not need to be labelled but DCJ may choose to do so. This should be the default position for newly created material, unless there is a specific need to protect the confidentiality or integrity of the information.

Any material which is not work related is considered 'UNOFFICIAL' and does not need to be labelled.

If OFFICIAL material requires specific handling or where disclosure may be limited or prohibited by legislation, the DLM must be applied to the document.

There are three protective marking paradigms which can be applied to a document:

- DLM
- security classification
- caveat

Paradigm	Description
DLM	• Sensitive information, if compromised, may cause damage to individuals, organisations or government. NSW uses six DLMs to describe the type of sensitivity of the information. DLM's adopted by DCJ as part of the NSW Government's system include: • OFFICIAL: Sensitive - NSW Cabinet • OFFICIAL: Sensitive - Legal • OFFICIAL: Sensitive - Law enforcement • OFFICIAL: Sensitive - Health information • OFFICIAL: Sensitive - Personal • OFFICIAL: Sensitive - NSW Government

Security Classification	Used to protect the most sensitive government information. The security classifications include: • PROTECTED • SECRET • TOP SECRET Each level of classification reflects the consequences of unauthorised disclosure and has strict handling and security clearance requirements. NSW agencies that handle information requiring security classification must manage this information in accordance with Commonwealth requirements. Security classifications PROTECTED, SECRET and TOP SECRET are to be regarded as national security classifications under these guidelines.
Caveat	The caveat is a warning that the information has special protections in addition to those indicated by the security classification. Caveats are not classifications and must appear with an appropriate security classification marked as text. The caveat is a warning that the information has special non-disclosure requirements in addition to those indicated by the protective marking. Caveats should not be used extensively in NSW. People who need to know will be cleared and briefed about the significance of information bearing caveats; other people are not to have access to this information. Caveats include: • codewords (sensitive compartment information) • foreign government markings • special handling instructions • releasability caveats

Application of classification and labelling must be in compliance with the DCJ Data Privacy and Protection Standard. This standard provides further information on which protective markings should be used in different circumstances and provides information on how to apply those protective markings.

Information with a DLM or security classification:

- may only be transferred across networks or copied to other media where the confidentiality and availability of the information can be reasonably assured.
- may only be disclosed outside the DCJ with the appropriate authorisation.

Documents that commit or oblige the DCJ in its business activities should be checked and countersigned (manually or electronically) to confirm their validity and integrity.

The NSW Government establishes that government information is to be open to the public. Information that must be released to the public is classified as 'open access information'. These include DCJ policy documents, register of government contracts and agency information guide.

All documents that are considered to be open access information must be first approved by a director or above.

Information should not be downgraded to a lower classification without undergoing a formal declassification effort sponsored by the information asset's delegated owner. The owner of the information must determine whether the information can be moved to a lower classification based upon the definitions of the classifications.

It is the responsibility of the information asset owner to monitor information assets and continuously review the information's classification. The information asset owner must determine whether an information asset's classification should be raised.

5.2 Secure information use

DCJ subscribes to a clear desk and clear screen principle, by which all information of a sensitive nature must not be left unattended whether working from home or in any other location. This should be achieved by:

- storing all sensitive physical information in locked cabinets or within document filing rooms when not in use — if the information is no longer required, the documents must be destroyed by placing in secure disposal bins or by shredding
- ensuring printed documents are collected as soon as they are printed
- practising caution when transferring information either in written or digital formats — transfer should be in accordance with the information's legal basis for sharing, classification and the inherent handling requirements
- not discussing or viewing highly sensitive information in public locations susceptible to eavesdropping
- locking IT devices when not in use
- wiping all sensitive information on whiteboards or work boards after use.

Destruction of media must be in compliance with the *State Records Act 1998* and the relevant disposal authority relating to the information. A link to the various State Archives & Records disposal authorities as they relate to DCJ information can be found at the following link: https://www.records.nsw.gov.au/recordkeeping/rules/retention-disposal-authorities. Consideration must also be given to the procedures identified within the DCJ Data Privacy and Protection Standard.

Information with a DLM or security classification can only be removed from DCJ premises on the following conditions:

- if the information is in a physical form (e.g. hardcopy document) prior written approval must be obtained from the appropriate manager
- if the information is in electronic form (e.g. data file) it can only be downloaded to external media / devices using approved technologies, otherwise prior written approval must be obtained from the appropriate manager.

Hard-copy material with a DLM or security classification that requires destruction must be placed in secure (locked) destruction bins, for secure disposal by approved contractors who hold a government security clearance.

Destruction of government information is to occur only with prior formal approval within the appropriate DCJ delegation and using approved disposal authorities.

The transfer of information via physical media (e.g. paper file, USB, CD) or electronic form (email, file transfer protocol) needs to be transferred in a manner consistent with the highest classification's protective controls as defined in the Data Privacy and Protection Standard.

Bulk transfers of sensitive unique records which convey information covered by the *Health Records and Information Privacy Act 2002* or *Privacy and Personal Information Protection Act 1998* must be encrypted. Intermittent transfers of singular or a limited numbers of these type of records should be encrypted but can be transferred without encryption as long as appropriate precautions are taken.

5.3 Sharing information

When sharing or disclosing information with an external entity, contracted non-government organisation, or other NSW Government agency as mandated by law, or there are reasonable grounds to believe the disclosure is necessary to prevent or lessen a serious and imminent threat to the life or health of a person, appropriate security consideration should be given to the disclosure. The requirements for ensuring the security of the information to be disclosed must be directly proportional to the sensitivity of the information and level of risk imposed by the sharing arrangement.

5.4 Outsourcing information

The outsourcing of DCJ information systems must undergo a risk assessment to appropriately ensure risks are managed prior to the information system being outsourced and the classification of the data residing in the outsourced solution.

All outsourcing or sharing contracts/agreements:

- must contain clauses that indicate the relevant entity will take all steps necessary to comply with State and Commonwealth privacy legislation as appropriate

- must have contemporary non-disclosure clauses which protect the privacy and confidentiality of DCJ information
- that the entity will be responsible for, in consultation with DCJ investigating, managing and resolving any data breaches and investigating, managing and resolving all complaints and reporting to the NSW Privacy Commissioner arising from its contravention of privacy legislation, including any complaints arising from data breaches.
- should be monitored regularly to ensure requirements are being met.

Where an external party is engaged to manage the transmission or storage of DCJ information, the arrangement for the collection, storage, access, use and disclosure of information must be in compliance with the *Privacy and Personal Information Protection Act 1998* and the *State Records Act 1998* and procedures identified within the DCJ Data Privacy and Protection Standard.

5.5 Protection of records

Standards for record retention, storage, handling, and disposal must comply with the *State Records Act 1998* for applicable information. The relevant disposal authority for this type of information must be defined and disseminated.

Should DCJ enter into a contract with an external entity which results in the transfer of devices to the external party, DCJ must:

- ensure all information as appropriate is stored in a records management repository prior to being wiped
- wipe the devices in line with the requirements from the data privacy and protection standard to ensure configuration files and information are not inadvertently provided to the external party.

6 Related legislation and documents

This policy supports adherence to:

- *Privacy and Personal Information Protection Act 1998*
- *Health Records and Information Privacy Act 2002*
- *State Records Act 1998*

7 Responsibilities

7.1 Compliance, monitoring and review

It is the responsibility of Cyber Risk Audit and Compliance team (CRAC) to monitor and update this policy annually or more frequently when any significant new information, legislative or organisational change warrants amendments to this document.

8 Document information

Document name	Data Privacy and Protection Policy
Applies to	All of DCJ with the exception of Judiciary members
Replaces	Data Privacy and Protection Policy V1.0
Document reference	D20/1977418
Approval	Deputy Secretary, Corporate Services 20 May 2021
Version	2.0
Commenced	20 May 2021
Due for review	May 2022
Policy owner	Chief Information Security Officer

9 Support and advice

You can get advice and support about this policy from the CRAC team who has carriage of this document.

Business unit	Cyber Risk Audit and Compliance Information Security Management Information and Digital Services Corporate Services
Email	FACSSecurityGovernance@facs.nsw.gov.au

This policy is subject to change. The latest published version of the policy is available on the DCJ Intranet.

If you need assistance identifying when you need to engage information security, please see

Appendix – Engaging information security.

For support, advice or further information contact:

Email	SecurityEngagement@facs.nsw.gov.au

10 Appendix – Engaging information security

The following questionnaire can be used to help you determine when you need to engage Information Security.

- Do you believe your password has become known to another party?
- Do you believe your computer has been infected with Malware?
- Have you just received a scam email?
- Have you seen something that breaches the Information Security Policy and need to report it?
- Have you become aware of a data breach and need to report it?
- Do you need a security investigation carried out?

If you answer yes to any of the above, please call or email

- **Former FACS Service Desk:** (02) 9765 3999 OR
- **Former Justice Service Desk:** (02) 8688 1111
- Legal: infoandprivacy@justice.nsw.gov.au

- Are you running or involved with a project which is implementing, updating or removing an ICT component?
- Are you running or involved with a project which has the potential to impact the confidentiality, integrity or availability of DCJ information, services or assets?
- Are you procuring a service from a third party which sees DCJ information being stored, used, created or processed by the third party?
- Are you sharing DCJ information with a non-DCJ party and require advice about whether this is lawful or require advice about an ICT risk assessment?

If you answer yes to any of the above, please email:

- **For former FACS staff**: FACSSecurityGovernance@facs.nsw.gov.au

- **For former Justice staff:** Information.Security@justice.nsw.gov.au
- Legal: Infoandprivacy@justice.nsw.gov.au