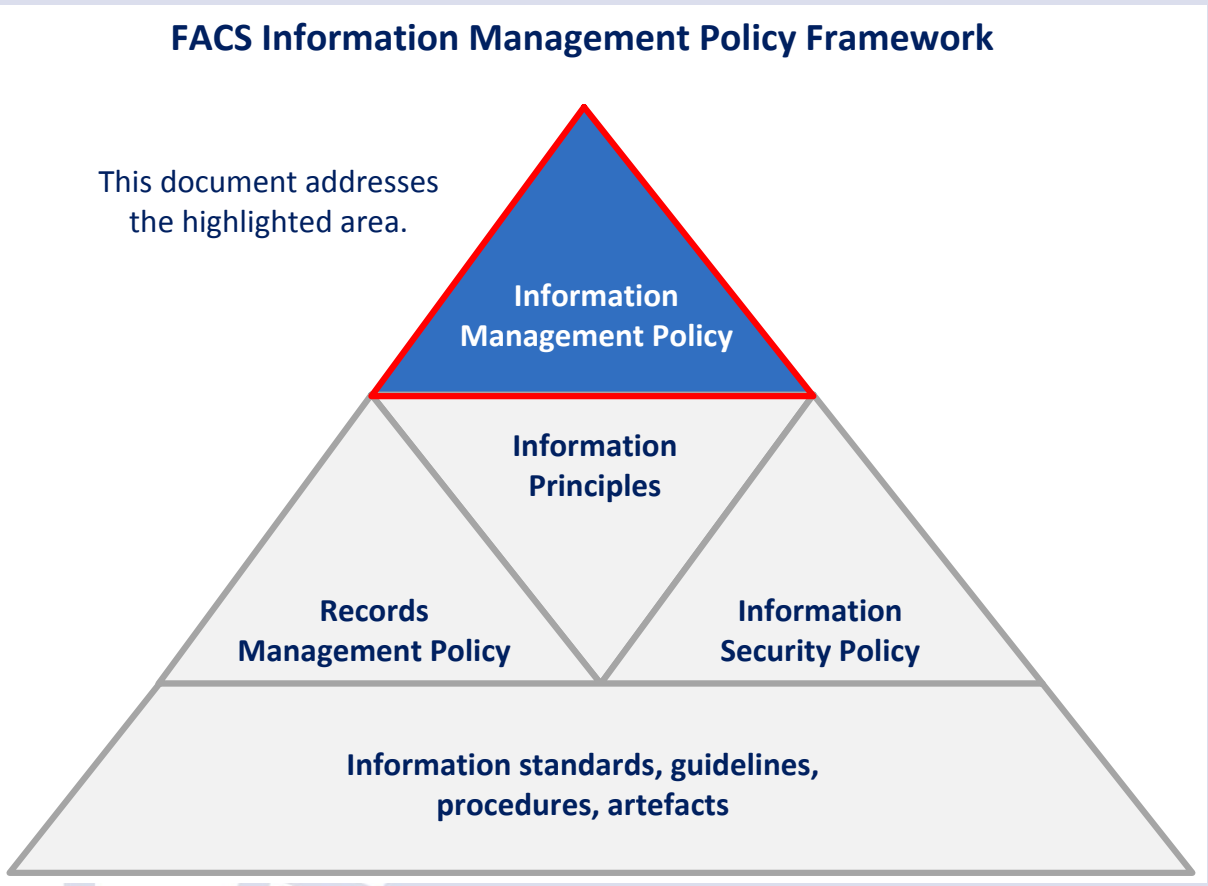
Information Management Policy

Summary: This Policy is designed to guide best practice information management



Document approval

The Information Management Policy has been endorsed and approved by:

Signature on file	Signature on file
Margaret Crawford	Tim Hume
Deputy Secretary Corporate Services	Chief Information Officer (CIO)
Approved: January 2016	Approved: January 2016

Document version control

Distribution:	All Staff
Document name:	Information Management Policy
Trim Reference:	D18/1059412 - AFACS/4079
Version:	Version 2.0
This document replaces:	Not Applicable
File name:	FACS Information Management Policy
Authoring unit:	ICT
Date:	July 2018
Next Review Date:	January 2019

Table of contents

1 Purpose of Policy

1.1 Purpose

The Information Management Policy and related information management governance documents are designed to guide the delivery of best practice information management within the Department of Family and Community Services (FACS) cluster.

The purpose of this Policy is to communicate the expectations, roles and responsibilities for staff to effectively manage FACS' information assets in all forms.

1.2 Background and policy links

Information is a fundamental and critical component for the provision and planning of services to some of the most disadvantaged individuals, families and communities in NSW. In order to effectively and efficiently deliver, plan and report on these services, information must be handled consistently and securely throughout its lifecycle. Public confidence in the ability of FACS to collect and manage information effectively and in line with our obligations requires application of the highest standards in information management practices.

The suite of documents below provide an Information Management Policy Framework for the Department to achieve effective, accurate and secure systems and processes (human and technical) for the benefit of clients and the broader community. It sets a clear expectation for FACS to work towards achieving best practices, productivity gains and improved business outcomes through improved information management. This Policy was developed in consultation with internal stakeholders.

The Information Principles are central to the Framework and provide overall guidance on the way FACS treats its information assets. The following documents are linked to the Information Management Policy:

- Information Principles
- Information Security Policy
- Records Management Policy

2 Definitions

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

Term	Definition
Custodian	The body or position designated with the custody of a specific dataset or information asset. The custodian is primarily responsible for: • The development, management, care and maintenance of a specified dataset or information asset • Ensuring that all legal, regulatory and policy requirements are met in relation to the management of the specified dataset or information asset; and • Determining the conditions for appropriate use, sharing and distribution of the specified dataset or information asset.
Data	The representation of facts, concepts and instructions in a formalised, consistent and agreed, manner that is suitable for communication, interpretation and processing by human or automatic means. Data is not information until it is used in a particular context for a particular purpose (Office of the Australian Information Commissioner (OAIC) 2013). Data is considered to be conceptually at the lowest level of abstraction.
Dataset	An identifiable collection of data. Most commonly a dataset corresponds to the contents of a single database table or a single statistical data matrix. The term can also be used to refer to the in a collection of closely related tables. A dataset may comprise a smaller grouping (or subset) of data which, though limited by some constraint or feature type, is located physically within a larger dataset.
Delegated owner	The position which has been delegated to have authority and accountability for an information asset.
Governance	Information governance is the system by which the current and future use of information and its management is directed and controlled through a system of policies, procedures, standards and guidelines.

Term	Definition
Information	Any collection of data that is processed, analysed, interpreted, classified or communicated in order to serve a useful purpose, present fact(s) or represent knowledge in any medium or form. This includes presentation in electronic (digital), print, audio, video, image, graphical, cartographic, physical sample, textual or numerical form (OAIC 2013). Information is typically considered to be at a higher level of abstraction than data.
Information Management Lifecycle	Describes the phases through which information passes, from initial collection, through organisation, usage, sharing and ultimately disposal.
Steward	Designs all rules and meta-data structures for the enterprise information asset(s) in accordance with the directions and requirements of the delegated information owners; responsible for establishing and maintaining the enterprise wide information base, including information models, taxonomies and vocabularies. An example of a type of steward role in the context of this Policy would be the Enterprise Information Architect.
User	End consumer of a data or information resource; those who use data or information for reference, or as input to solve problems and/or make decisions.

3 Scope and application

This Policy is to be followed by all FACS employees including full-time and part-time, casual and temporary employees, contractors, consultants, students and volunteers, and any other parties who have access to FACS' information assets and associated information processing facilities.

This Policy applies to information related to business conducted by FACS in all forms including digital and hard copy, data and information systems.

This Policy should be read in conjunction with the Information Principles, Information Security Policy and the Records Management Policy.

4 Legislation

The legislative and government requirements which apply to this Policy include:

- Privacy and Personal Information Protection Act 1998
- Government Information (Public Access) Act 2009
- Health Records and Information Privacy Act 2002
- Public Finance and Audit Act (s11)
- Public Sector Employment and Management Act 2002
- Children and Young persons (Care & Protection) Act 1998
- National Classifications of Community Services V2.0 (2002)
- NSW Treasury Policy & Guidelines Paper TPP 15-03 - Internal Audit and Risk Management Policy for the NSW Public Sector
- State Records Act 1998 including standards and retention and disposal authorities under the Act
- State Records Regulations 2010
- Electronic Transactions Act 2000
- Australian Standard Records Management AS ISO 15489-2002
- AS/NZS ISO/IEC 27001 Information technology - Security techniques - Information security management systems – Requirements
- AS/NZS ISO/IEC 27002 Information technology - Security techniques - Code of practice for information security management
- AS/NZS ISO 31000 Risk management - Principles and guidelines.

5 Policy statement

Managing information effectively and appropriately is essential to the delivery of secure, seamless and efficient operational services. It provides the basis for informed decision making and the platform upon which performance can be measured. FACS plays an important role in improving the lives of vulnerable people in NSW. In the work that we do, we regularly handle information regarding some of the most disadvantaged and vulnerable individuals, families and communities in the State. It is vital to value and protect FACS' information, information systems and information resources.

Under this Policy FACS is committed to ensuring that:

- Information is valued as an asset which is fundamental to the efficient and effective delivery of public services

- FACS' Information Management Principles are embedded into all aspects of business activities (refer Information Principles. Version 1.0, September 2015, NSW Government, FACS)
- Effective governance of information assets is established and maintained including identifiable information owners for key assets
- All information, in all formats and media, is securely and appropriately managed through the different stages of its lifecycle
- There is compliance with all relevant legislation and standards
- Information is available and shared with people have a business need to know
- Wherever possible information is collected and recorded only once to ensure a single authoritative source of that information
- Information is of sufficient quality to meet the purpose for which it is intended
- Information is recorded and made available in standardised forms (that is, format, content and concepts) and is linkable to other information to enhance its value and opportunities for re-use
- There is a proactive approach to the release and publication of information for wider consumption in line with government open data principles; and
- Information is retained and archived in line with regulatory requirements.

Access to information by clients and community members is reinforced through support for FACS access application processes under the *Government Information (Public Access) Act 2009* (GIPA), *Privacy and Personal Information Protection Act 1998* (PPIPA), and *Health Records and Information Privacy Act 2002* (HRIPA).

6 Roles and responsibilities

The main roles and responsibilities for the implementation of this Policy are described in this section including the custodianship of a specified dataset or information asset.

Refer to:

- NSW Data and Information Custodianship Policy, Version 1.1, June 2015, NSW Government
- Information Management Responsibilities and Accountability GUIDANCE, June 2013, NSW Government; and
- NSW Government: Information Management: A common approach, Version 1.2, July 2015, NSW Government.

6.1 The Secretary

The Secretary is responsible for:

- ensuring that FACS complies with all relevant NSW Government legislation and standards relating to information management.

6.2 Chief Information Officer (CIO)

The CIO is responsible for:

- leading a quality management approach to information management; and
- ensuring that this Policy is incorporated into the Information and Communication Technology (ICT) Governance Framework and structures.

6.3 Director, Information Management

The Director, Information Management is responsible for:

- providing the oversight of the maintenance and review of this Policy
- oversees the creation, publication and maintenance of related guidance documents for all staff
- ensures that this Policy is:
    - applied to all new initiatives (developments and acquisitions) involving the capture and the use of information
    - pragmatically applied to the legacy information environment
- provides expert advice at the strategic business and operational levels.

6.4 Director, ICT Governance Security and Risk

The Director, ICT Governance Security and Risk is responsible for:

- conducting risk assessments against information systems and processes
- provision of mitigation plans to control risk; and
- supporting delegated owners and custodians in achieving security compliance requirements.

6.5 Enterprise Architect

The Enterprise Architect acting in the role of steward is responsible for:

- defining the information and related data structures, the vocabularies, the business rules, procedures and classification schemes with an enterprise wide focus, to conform with established standards and the business requirements of all delegated owners

- building and maintaining all information architectural artefacts and models
- provide advice on, and oversight on the implementation of information and related data artefacts, whether electronic or otherwise
- take custody of information management (information, records, information security and data) policy, standards, guidelines, governance, procedures manuals, etc., and maintain the enterprise-wide repository of information architecture artefacts and all reference material. This includes its distribution, backup and archival, and all security aspects where appropriate
- monitor and report all non-compliance with the Information Management Framework (policies, etc.) to delegated owners and escalate to the Information Governance Board; and
- examine and recommend the approval of requests for dispensation from established information management policies to a designated level of delegation, and assume responsibility for accepting any consequent residual (mitigated) risk. Where required, escalate such requests to delegated owners or the Information Governance Board for their decision and resolution.

6.6 Chief Technology Officer (CTO)

The CTO is responsible for:

- the provision of the IT infrastructure and resources required to ensure successful operation of the information management systems
- resourcing and supporting the technical implementation of the information management system
- developing and testing the Business Continuity Plans (BCP) for the information management systems
- assists with information and data migration, de-commissioning and disposal initiatives
- implementing the required information security and access requirements according to business needs, legislation and regulatory requirements and whole-of-government policy
- implementing records access and security requirements according to business needs, legislation and regulatory requirements and whole-of-government policy
- administering and maintaining the information systems for corporate services; and
- test and audit information systems to ensure that they are operating routinely and that there are no issues affecting information and data integrity, usability or accessibility.

6.7 Delegated Owner

The Delegated Owner is responsible for:

- taking possession and overall control of the information asset
- is accountable, and liable, for the information asset
- has authority over the security, quality and appropriate disposition of the asset
- approves the business rules pertaining to the information asset
- establishes access conditions to the information asset, including:
    - open access licensing and disposition; and
    - formal agreements with value-adding agencies (e.g. funded providers such as non-government organisations (NGOs) and other government agencies).

6.8 Custodian

The Custodian is responsible for:

- the security, quality and appropriate disposition of the information asset
- manages and aims to control any risks associated with the information asset
- maintains the validity of the datasets and information assets
- manages and maintains data, including metadata, to ensure that discovery mechanisms function
- ensures that with access to the data, the metadata is also available and that it is discoverable, accessible and current
- ensures that datasets conform to appropriate agreed standards
- develops and regularly reviews the conditions and processes under which individual datasets are made available, for example by licences or proactive release
- establishes, monitors and maintains standards relevant to pricing and access to data
- manages storage, maintenance, security and archival procedures
- cultivates community awareness
- provides advice on the proper use and interpretation of data
- nominates a single point of contact for customer enquires in relation to the dataset
- ensures that all legal, regulatory and policy requirements are met in relation to the management of the specified dataset or information asset; and

- determines the conditions for appropriate use, sharing and distribution of the specified dataset or information asset.

6.9 All Managers

All Managers are responsible for:

- supporting and fostering a culture of good information management practices in accordance with the FACS Information Management principles; and
- ensuring that staff are trained or briefed and aware of their responsibilities for pertaining to information management.

6.10 All Staff (including Students and Volunteers)

All Staff are responsible for complying with this policy by:

- ensuring the recording of information into our information systems are in line with procedures and guidelines; and
- upholding the security and privacy of information retained in the information systems they have access to.

7 Monitoring, evaluation and review

It is the responsibility of Information Management, ICT to monitor and update this Policy as required.

This Policy will be reviewed on a yearly basis and or when any significant new information, legislative or organisational change warrants amendments to this document.

Reviews will be completed in consultation with the appropriate information management stakeholders for relevance and effectiveness.

8 Support and advice

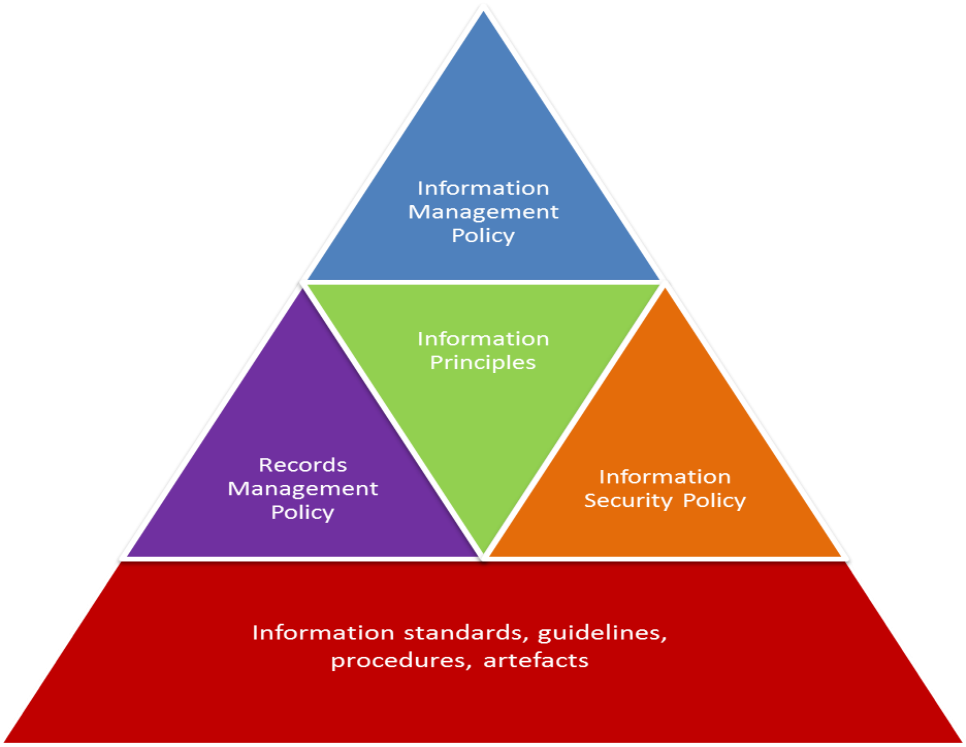
Please contact infomgmt@facs.nsw.gov.au for support and advice regarding this Policy.

If you are reviewing a printed version of this document, please refer to the intranet to confirm that you are reviewing the most recent version. Following any subsequent reviews and approval, this Policy will be uploaded to the intranet and all previous versions removed.

Appendix A: FACS Information Management Policy Framework

The FACS Information Management Policy Framework is a system of policies and supporting standards, guidelines and procedures that embody a set of principles, guiding the way in which we treat and manage our information assets.

Diagram 1: Information Management Policy Framework



Central to the Framework is the set of principles for information management (see Information Principles, Version 1.0, September 2015, FACS).

FACS' policies with respect to information are derived from these principles and grouped into three inter-related yet distinct categories:

- Information Management Policy (this document) - the overarching policy
- Records Management Policy – separately defined due to specific legislative and compliance requirements; and
- Information Security Policy – separately defined due to specific legislative and compliance requirements.