GAWLER RIVER FLOODPLAIN MANAGEMENT AUTHORITY

INFORMATION ASSET MANAGEMENT MANUAL

Incorporating the

INFORMATION ASSET MANANGEMENT PROGRAM,

PLAN, POLICY and PROCEDURES

Adelaide Hills Council
Adelaide Plains Council
The Barossa Council
Gawler
Light Regional Council
City of Playford

GAWLER RIVER FLOODPLAIN MANAGEMENT AUTHORITY

Address: 266 Seacombe Road Seacliff Park, South Australia 5049
Telephone: 0407 717 368
Email: eo@grfma.com
Website: www.gawler.sa.gov.au/grfma

1. INFORMATION ASSET MANAGEMENT MANUAL

Strategic Reference:	Information Asset Management
File Reference:	GRFMA, 7.0 Information Asset Management, 7.1 Manual
Responsibility:	Executive Officer
Applicable Legislation:	State Records Act 1997, Freedom of Information Act 1991, Local Government Act 1999, GRFMA Charter 2020
Related Policies/Codes:	Access to Meetings and Documents Policy Freedom of Information Statement
Related Procedures:	As approved by the Executive Officer and included in this Information Asset Management Manual containing the Information Asset Management Program and Plan
External Regulations	Local Government Act 1999 State Records Act 1997 Freedom of Information Act 1991
Adopted:	17/10/2024
Minutes Reference:	GB59/24
Revision Number:	1
Frequency of Review:	Annual as part of the Self-Assessment and Reporting Process
Next Review Due:	October 2025

CONTENTS

ACRONYMS AND DEFINITIONS 5

INFORMATION ASSET MANAGEMENT PROGRAM 7

1. INFORMATION ASSET AUDIT 9

2. VALUE AND RISK ASSESMENT 11

3. INFORMATION ASSET MANAGEMENT PLAN 14

3.1 POLICY and PROCEDURES 14

Information Asset Management Policy v1 (GB85/23) 14

1. Introduction 14

2. Scope 14

3. Policy Statement 14

4. Principles 14

5. Resourcing 17

6. Planning 17

7. Review 17

Information Asset Business Classification, Titling and Filing Procedures 18

1. Introduction 18

2. Scope 18

3. Background 18

4. Procedures 18

5. Business Classification Scheme 20

6. Sustainable Digital File Formats 20

7. Risk Assessment 21

Information Asset Digitisation Procedures 22

1. Introduction 22

2. Scope 22

3. Background 22

4. Procedures 22

Information Asset Disposal Procedures 24

1. Introduction 24

2. Scope 24

3. Background 24

4. Procedures 25

Digital Signature Procedures 29

1. Introduction 29

2. Scope 29

3. Background 29

4. Procedures 29

3.2 DEFINED RESOURCES, ROLES AND RESPONSIBILITIES 30

3.3 ACCESS AND RELEASE SCHEMES 30

3.4 SECURITY CONTROLS 31

3.5 PRIVACY PROTECTION AND CONSIDERATIONS 32

3.6 DISPOSAL DETERMINATIONS 32

3.7 COMPLIANT SYSTEMS 33

4. EDUCATION 33

5. SELF-ASSESSMENT AND REPORTING 34

Appendix A: NAP Guidelines - Destruction of Unofficial Records 35

Appendix B: Business Classification Scheme 37

Appendix C: Risk Assessment Matrix 38

Appendix D: Disposal Authorisation Proforma 42

ACRONYMS AND DEFINITIONS

Access Derivatives	Compressed copies of the **Digitised Hard Copy Information Asset** created for dissemination and access
Authority	Gawler River Floodplain Management Authority
ASP	Approved Service Provider (as approved by SRSA)
BCS	Business Classification Scheme is a structure for arranging and managing information assets according to their function, activity and retention period (value).
Compromise	Includes, but not limited to, loss, misuse, interference, unauthorised access, unauthorised modification, unauthorised disclosure of **Information Assets**
Converted	**Hard Copy** (physical) **Information Assets** that have undergone a process of change from analogue to a permanent digital format.
Digitised	A hard copy information asset that has undergone a scanning process, resulting in conversion to a digital format, either for access (derivative) or preservation (surrogate) representation.
Disposal	The process of either permanently destroying or transferring custody or ownership of information assets.
EDRMS	Electronic Documents Records Management System. Software applications designed specifically for the management of collated information assets and items.
EO	Executive Officer
FOI	Freedom of Information
GDS	General Disposal Schedule
Hard Copy	Physical information assets as opposed to digital. The term is used in relation to digitisation. Previously referred to as “hard copy source records”, the preferred term is “physical **information assets**”.
In Place	The practice of managing information assets within the software application where they are created as opposed to transferring to a dedicated **EDRMS.**
Information Asset (IA)	Includes data and records in any format, where it is created or received through the conduct of the Authority’s business. Usually applies to a series or system rather than an individual **Item**.

IAM	Information Asset Management
ICT	Information and Communication Technology
Item	A single **Information Asset** (physical or digital) of evidential value to the Authority. The term **Item** is used to distinguish from a series, collection or data sets managed **In Place** rather than within a dedicated **EDRMS**.
Master	Applied to the original or permanent version of an **Item**. Particularly used to refer to the **hard copy** source record that has been **digitised** and retained for as long as needed as digitisation process and digital storage are not fully compliant with SRSA Standards. Master versions must not be destroyed until after the minimum retention period has been reached.
NAP	Normal administrative Practice
Plan	Information Asset Management Plan
Program	Information Asset Management Program
RADL	Records Access and Description List
SRSA	State Records of South Australia

INFORMATION ASSET MANAGEMENT PROGRAM

Collectively, these elements will assist in developing a clear strategic direction for the management of information assets as well as foster a good information management culture with a view towards continuous improvement.

A Program should support broader strategic and corporate goals and objectives, carrying the same executive level commitment.

The following steps, in any order, assist to develop and implement a Program:

1. Information Asset Audit

Undertake an information asset audit to identify what information assets are held. The identified information assets must be linked back to the business activities and functions.

2. Value and Risk Assessment

Assess and value what information assets should be created to support an agency's business and regulatory requirements. To do this, consider legal and regulatory requirements, associated risks and business objectives.

Identify and manage risks associated with not creating information assets to support requirements. This can be achieved by undertaking a value and risk assessment.

3. Information Management Plan

A Plan provides practical direction for implementing a Program. The Plan should be based on the outcomes of the information asset audit and value and risk assessment and identify information priorities.

4. Education

Induct and train staff on the Program. A large part of the success of a Program relies on the commitment of staff to information management policies and procedures and an awareness of their information management responsibilities.

Educating staff in the value and management of information is key to fostering a culture of good information management.

5. Self-assessment and Reporting

Continue to formally assess and review the Program using the Self- Assessment Tool (Tool). This assessment can also assist agencies to understand gaps in their Program and can be used as a first step in the review of the Program.

1. INFORMATION ASSET AUDIT

All the Authority's digital information assets are stored and managed within **M365** (Basic Business licence). Physical information assets are stored and managed in a **Physical** filing system. All information Assets must be handed over to the Authority or the Authority's representative at the termination of the Executive Officer's Contract.

The Executive Officer and other Contractors are likely to utilise a range of software applications (business systems) to manage activities or tasks. Examples include MYOB for financial management and Adobe DC Pro for digital signatures (DocuSign). Licences for these software applications are the responsibility of the Contractor who will ensure that all required information assets such as reports, data sets and signed documents are captured into the Authority's OneDrive for management. Outgoing Contractors must ensure that all relevant data is exported from software applications in an accessible and useable format, to be retained for as long as needed with the capability of being imported into another compatible software application.

Further details are included in the *Information Asset Control Register* sheet 'Audit' (Excel).

Information Assets	BCS	Locations	Owner/Administrator
Board and Committee proceedings including agenda, supporting documents and minutes.	1.0 Board and Committees	M365 / Physical / SRSA	GRFMA / EO
Annual Reports and material produced for public information.	2.0 Publications	M365 / SRSA	GRFMA / EO
Dam proposals, construction, inspection and maintenance including plans, maps, reports and images.	3.0 Infrastructure Management	M365 / SRSA	GRFMA / EO
Accounting including invoices, Profit & Loss Reports, Budgets Audit Reports	4.0 Finance	M365 / Physical	GRFMA / EO
Asset management, long-term financial and strategic management plans	5.0 Strategic Management	M365	GRFMA / EO

Routine operational items including enquiries, drafts, planning and preparation of budgeted activities, managed in subject files.	6.0 Admin	M365	GRFMA / EO
Member case files including applications, declarations and inductions	6.1 Member Management	M365	GRFMA / EO
IAM Manual, Control Register, Self-Assessment, SRSA survey Responses, Destruction Authorisations, Reports, SRSA Transfers (including proposals, series and consignment descriptions and transfer receipts),	7.0 Information Asset Management	M365	GRFMA / EO

2. VALUE AND RISK ASSESMENT

Value of assets increases when the consequence of not creating, retaining and managing securely increases. Risk is measured based on the consequences of non-compliance with internal operational needs and external legislative requirements. The Risk Assessment Matrix is included as Appendix C.

In addition to the requirements of the Local Government Act and GRFMA Charter, under the State Records Act 1997, Part 5, Clause 16, inadequate information asset management may be reported to the Minister and intentional unauthorised destruction or damage to information assets incur a maximum penalty of $10,000 or 2 years imprisonment (Clause 17).

Further details are included in the *Information Asset Control Register* sheet 'Audit' (Excel).

Information Assets	BCS	Business Objectives	Legislative/Regulatory Requirements	Associated Risks with not creating and retaining	Risk Rating
Board and Committee Proceedings	**1.1 1.2 1.3**	Document decision making, ensuring accountability and historical reference.	Local Government Act 199, Schedule 2. State Records Act 1997, Part 5	Lack of accountability and documented evidence of decision making. Inadequate information asset management.	**Extreme Risk**
Annual Reports	**2.1**	Summary of activities of the past year provides public transparency, retained permanently for accountability and historical purposes.	Local Government Act 199, Chapter 8 Administrative and financial accountability. State Records Act 1997, Part 5	Lack of compliance and summary for historical evidence. Inadequate information asset management.	**High Risk**

Other Publications	**2.2**	Ad hoc presentation of information for public consumption	Open Data Principle	Lack of proactively releasing information on activities and progress with projects.	**Low**
Infrastructure Management	**3.1** **3.2** **3.3** **3.4**	Documenting the process of construction and management of significant infrastructure requiring ongoing active management.	LGA Schedule 1A Environment Protection Act Native Title Act, SA 1994 / Cth 1993 Native Vegetation Act 1991 Natural Resources Management Act 2004 Water Resources Act 1997 Planning, Development and Infrastructure Act 2016 State Records Act 1997, Part 5	Lack of compliance, accountability, evidence and information required for ongoing management leading to series consequences including potential loss of life. Inadequate information asset management.	**Extreme Risk**
Finance	**4.0**	Financial accountability and management of funds for current and long-term sustainability.	Local Government Act 199, Chapter 8 Administrative and financial accountability. State Records Act 1997, Part 5	Lack of compliance, accountability, evidence and information required for ongoing management. Inadequate information asset management.	**High Risk**
Strategic Management	**5.1** **5.2** **5.3** **5.4**	Planning for ongoing sustainability of fiscal assets and infrastructure.	Local Government Act 199, Chapter 8 Administrative and financial accountability. State Records Act 1997, Part 5	Lack of compliance, accountability, evidence and information required for ongoing management. Inadequate information asset management.	**High Risk**

Admin	**6.0**	Operational planning and routine business activities	GRFMA Charter, Chapter 10 State Records Act 1997, Part 5	Lack of documented activities resulting in poor operational management, lack of evidence and inadequate information asset management.	**High Risk**
Member Management	**6.1**	Manage Member appointments, declarations and inductions.	LGA - Chapter 5, Part 4 Privacy Act 1988 (Cth) State Records Act 1997, Part 5	Lack of accountability, compliance and evidence of activity. Inadequate information asset management.	**High Risk**
Information Asset Management	**7.1** **7.2** **7.3** **7.4** **7.5**	IA Control, ensuring documented creation, classification, management and disposal according to endorsed policy and procedures.	State Records Act 1997, Part 5 State Records Act 1997, GDS 40 Libraries Act 1982 ISO 15489 Records Management	Lack of accountability and evidence of activity. Inadequate information asset management.	**High Risk**
All information assets		Managing in M365 rather than system full compliance with SRSA *Managing Digital Records in Systems* Standard.	State Records Act 1997, Part 5, Section 14(2)	Compliance SRSA Standards, although ideal, is not required by Local Government Authorities	**Low**

3. INFORMATION ASSET MANAGEMENT PLAN

3.1 POLICY and PROCEDURES

Information Asset Management Policy v1 (GB85/23)

1. Introduction

It is the aim of this policy to establish the roles, responsibilities, and requirements of the Authority as a manager of government information assets, as required by:

- The State Records Act 1997.
- Approved Information Management Standards, Schedules and Guidelines as issued by State Records South Australia.
- The Local Government Act 1999.
- The Gawler River Floodplain Management Authority Charter (28/01/2020).

2. Scope

This policy applies to the Authority including its Board members, Executive Officer and employees including volunteers and contractors.

3. Policy Statement

The Authority recognises the value of managing information assets effectively, accountably, and strategically, understanding the explicit link between information assets and information technology. This approach underpins both good governance principles and business success.

The Authority will provide efficient and appropriate access to information assets and ensure they are managed and disposed of in accordance with Standards, Schedules and Guidelines approved by State Records of South Australia (SRSA), under the State Records Act 1997 (SA).

To support this intent, the Authority will provide appropriate resources and training to successfully meet its commitment to the planned management of information assets.

4. Principles

The Authority recognises and applies the following principles and behaviours:

4.1 The value of information is known. Information is treated as an asset of the Authority. Its value to enable business activities and functions, both current and future, is determined, understood and leveraged to improve business outcomes.

The Authority will:

4.1.1 identify and document what its information assets are, where they are stored and who is responsible for their management;

4.1.2 understand and document how its information assets support its business objectives, operations and compliance obligations:

4.1.3 ensure information assets are linked to business functions and activities;

4.1.4 induct and train staff in the value of information and in their information asset management responsibilities; and

4.1.5 foster an organisational culture that values and manages information as an asset that supports business objectives, decision making and activities.

4.2 Information assets are created and managed appropriate to risk. The Authority understands what information needs to be created and maintained to support business objectives, drive decision making and meet compliance obligations. In doing so, business risks are mitigated.

The Authority will:

4.2.1 analyse and document what information assets must be created and managed across the organisation applicable to the regulatory environment in which it operates;

4.2.2 develop and issue policy and procedures outlining how information assets will be managed;

4.2.3 assess the risks of not creating or managing information assets where there is a legal, evidential, or business need;

4.2.4 manage information assets digitally unless there are specific reasons for keeping physical formats;

4.2.5 design and implement systems according to relevant standards so that they support the effective management and disposal of information assets;

4.2.6 manage and store information assets appropriately, to ensure they remain secure and accessible for as long as need;

4.2.7 only dispose of information assets in accordance with current, approved disposal determinations issued by State Records;

4.2.8 review and audit how well its information asset management policy, procedures and practices support its business, and

4.2.9 monitor, report and improve staff adherence to the internal Information Asset Management Program, including policy and procedures.

4.3 Ownership of information assets is assigned. Responsibility for the governance of information assets is assigned appropriately to ensure information assets are managed for the best outcomes of the Authority, its customers and the broader community.

The Authority will:

4.3.1 ensure ownership of information assets are assigned;

4.3.2 ensure that owners are aware of their responsibilities and accountabilities for managing the information assets;

4.3.3 ensure responsibilities for information assets management are delegated appropriately, in writing;

4.3.4 ensure that roles and responsibilities relating to the ownership and management of information assets are defined in policy, procedures and the Information Asset Management Program and the Information Asset Management Plan; and

4.3.5 ensure that ownership and accountability for information assets is managed consistently through a governance structure.

4.4 Information assets can be relied upon. Policy, procedures, practices and systems are implemented to ensure information assets can be relied upon as trusted and authentic evidence of decisions made and actions taken.

The Authority will:

4.4.1 make and keep full and accurate information assets, appropriate to its business processes, regulatory environment and accountability requirements to mitigate risk;

4.4.2 ensure information assets are saved into systems in a timely manner, that meet relevant SRSA Standards[1], the SA Protective Security Framework (SAPSF) and the SA Cyber Security Framework (SACSF), to ensure they are protected from compromise;

4.4.3 record relevant details (metadata) in systems so that the business context of information assets can be readily understood;

4.4.4 use established and existing definitions for information assets where possible, so that there is consistency across the Authority; and

4.4.5 implement practices and systems that ensure the quality and authenticity of information assets.

4.5 Information assets are accessible for as long as needed and are shared appropriately (subject to access, security, and privacy rules) within a protected and trusted environment.

The Authority will:

4.5.1 implement information security classifications and requirements that are applicable to the sensitivity of the information in accordance with whole of government policies and administrative directions;

[1] Standards include *Managing Digital Records in Systems*; *Minimum Recordkeeping Metadata Standard*, *Contracting and Information Assets Standard*; and *Management and Storage of Temporary Value Information Assets Standard.*

4.5.2 review access restrictions on information assets and amend as sensitivity alters;

4.5.3 migrate digital information assets as systems, software and media are upgraded or become obsolete, to ensure they remain accessible for as long as needed;

4.5.4 identify requirements for retaining information assets not covered by general disposal schedules, and seek a disposal determination for these information assets;

4.5.5 ensure that no information asset is destroyed unless no longer needed for business purposes and in accordance with current, approved disposal determinations;

4.5.6 collect, use, disclose, store, and dispose of personal information in accordance with the information privacy principles;

4.5.7 share information assets across government as appropriate and where authorised;

4.5.8 proactively publish information in line with government policy; and

4.5.9 not sell, abandon or donate information assets to external parties where such action would result in the agency not having access to that information and without authorisation in the form of a disposal determination.

5. Resourcing

With limited resources, no employees and one external consultancy, the Authority endeavors to maintain its Information Asset Management Plan by allocating resources within its budget and engaging appropriately skilled Consultants as required.

6. Planning

The Authority recognises the importance of planning the management of its information assets at an agency-wide level. The Information Asset Management Program supports the Authority's broader strategic and corporate goals and objectives through the framework of policy, procedures, education, technology and the Information Asset Management Plan which provides practical direction. Integral to planning is the SRSA Information Governance Guideline and Self-Assessment Tool (Tool) used to identify gaps and review the Program.

7. Review

7.1 This Policy shall be reviewed by GRFMA every three years.

7.2 Upon review, GRFMA will communicate the updated Policy to all relevant persons.

Information Asset Business Classification, Titling and Filing Procedures

1. Introduction

This Procedure covers the business classification, titling and filing of temporary, long-term and permanent value information assets created, received and held by the Authority.

This Procedure ensures consistency in the description of information assets and provides a link to the Authority's business functions and activities. Consistency in classification and descriptive terminology facilitate efficient retrieval, management and disposal of information assets.

2. Scope

This Procedure is applicable to the descriptive classification, titling and filing of all temporary, long-term or permanent value information assets, undertaken by the Authority contractors, employees and third parties as a routine administrative process.

3. Background

Most of the Authority's information assets are now created and received in digital format, however ad hoc physical records, such as invoices and correspondence, may continue to be received, resulting in hybrid information asset management. Some information assets will have short-term retention periods, others may require permanent retention.

This Procedure, and the entire *IAM Manual* complies with the requirement to document IAM behaviours in relation to the *Information Asset Management Policy (GB85/23)* principles, meeting SRSA Standards to the extent where risk mitigation is maximised in relation to the resources available to the Authority and the context with which it operates.

4. Procedures

4.1 Consistency - Apply the Business Classification Scheme, titles and file locations consistently.

Locations include email Inbox folders, MS365 One Drive digital folders, physical files and business systems such as MYOB.

Save in a digital folder or file in a physical folder, as appropriate, and title using hierarchical terminology from the general to the specific. Folder titles form the first part, or highest level of the hierarchical title. Sub-folder titles describe a more specific level with the file title providing the most specific description.

Applying the date in reverse format (yyyy.mm.dd) at the beginning of the file title will ensure items appear in chronological order. Decide on applying either date issued, date due or date paid and

consistently apply for the folder contents. Be consistent with the method of applying the date. For example:

GRFMA>Finance>Invoices 2024>2024.04.30 XYZ Services

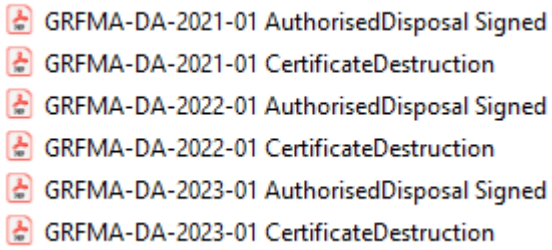
Folders containing multiple subjects can be arranged firstly in alphabetical order then chronological order by applying the date at the end of a constantly applied descriptor. Using this titling method will display the correspondence Received immediately above the Reply (alphabetically, Received comes before Reply). For example:

GRFMA>Administration>Correspondence>DoxLite IAM Manual Received 2024.05.28

GRFMA>Administration>Correspondence>DoxLite IAM Manual Reply 2024.06.07

GRFMA>Administration>Correspondence>DoxLite MS365 Received 2024.06.03

Another example of consistent titling is applying an identifier at the start of the title then consistent descriptors that will keep the related items in order. The example below shows the two related documents required for annual information asset destruction:



4.2 Emails - Digital files will often be received via email which can be saved to appropriately titled Inbox Folders. No further action is required for short term, facilitative messages which can be deleted under Normal Administrative Practice (see Appendix A).

For emails that contain decisions, instructions or other official business, save the email, including any attachments in .msg format, in the appropriate MS365 OneDrive digital folder. This will allow the .msg file to be opened in the email client from which it originated (e.g. MS365 Outlook). Saving the email as a .pdf (print or export to PDF) allows the file to be opened without the email client application but means that email attachments must be saved separately.

For emails with attachments where the body of the email does not contain official business information, save the attachments in .pdf (or the appropriate file format from the list in section 7. Sustainable File Formats). The email can then be moved to the appropriate Inbox Folder for quick access.

4.3 Physical records may be scanned then processed as a digital record with the original physical record filed and managed as the Master version. Retaining the physical version for the minimum retention period as identified in GDS 40 (as amended) removes the need to meet the requirements of GDS 21 (as amended) which allows for the early destruction of hardcopy source records after scanning,

according to documented specifications, quality assurance and saving into a business system which has been certified as compliant with SRSA Standard *Managing Digital Records in Systems.*

5. Business Classification Scheme

Functions, the highest descriptive level in the Business Classification Scheme, and their relationship to GDS 40 and retention requirements are listed in the table below. Activities are included in the full Business Classification Scheme in Appendix B and in the *Information Asset Control Register*, sheet 'BCS' (Excel)

Business Classification Scheme	Code	GDS 40 Class	Retention Period
Board & Committee	**1.0**	3.1	Permanent
Publications	**2.0**	5.3 and 100.6	Permanent
Dam / Infrastructure Management	**3.0**		Indefinite / Permanent
Finance	**4.0**		Temporary
Strategic Management	**5.0**		Temporary when Plans are included in Board Agenda Items
Administration	**6.0**		Temporary
Information Asset Management	**7.0**		

6. Sustainable Digital File Formats

The Authority is responsible for ensuring that information assets remain available and useable for as long as needed – at least as long as the minimum retention period. This can be achieved by ensuring that digital information assets are saved in a sustainable format and converted or migrated to new systems as technology changes. Sustainable file formats include those which are:

- widely used and supported
- identifiable and well documented
- independent of specific software, developers or vendors
- stable (rare releases of newer versions) and backwards and forwards compatible with other versions
- uncompressed or use lossless compression
- metadata friendly or have the ability to embed metadata.

Use sustainable formats when:

- creating new records and information

- converting or migrating records
- considering the file formats of any new software applications or design requirements when developing or implementing new systems
- requesting files or data sets from a cloud service provider.

Sustainable file formats include:

Audio files	.mp3 and .mp4
CAD (Computer-aided Design)	.dxf
Data Files and Databases	.csv and .xml
Email – as single messages including attachments	.msg and .eml
Encapsulation	.zip
Image files	.tif and .jpg
Office (Microsoft Office Suite)	.docx, .xlsx, pptx,
Text only	.txt, .csv and .xml
Video	.mpg, .mp4, mjp2,
Websites	.html, .htm, .xml and .warc (for archived websites)

7. Risk Assessment

This procedure applies to managing information assets in digital and physical folder structures, aligned to the BCS, rather than a software application specifically designed for IAM such as an EDRMS. Under the State Records Act 1997, Local Government Authorities are not required to comply with SRSA Standards, however compliance with disposal schedules in mandatory. Compliance with GDS 20 for the early destruction of digitised hard copy source records can only be achieved with compliance to the following:

- *Managing Digital Records in Systems Standard*
- Minimum Recordkeeping Metadata Standard

Non-compliance with the above Standards simply means that physical information assets must be retained for the minimum retention periods prescribed in GDS 40 as amended, even after scanning and saving into the M365 OneDrive digital folder structure.

Knowingly damaging, altering or disposing (destroying, selling or donating) of official records may result in a penalty of $10,000 or imprisonment for 2 years (State Records Act 1997, Section 17(1).

The Risk Assessment Matrix (Appendix C) has been utilised to determine risk ratings associated with not complying with internal and external requirements to create, retain and manage information assets. Under the State Records Act 1997, Local Government Authorities are not required to comply with Standards issued by SRSA, although doing so is ideal where practical given sufficient size and resources.

Information Asset Digitisation Procedures

1. Introduction

This Procedure covers the digitisation of temporary, long-term and permanent value, hardcopy source records created, received and held by the Authority, to facilitate workflows.

This Procedure does not allow for the destruction of hardcopy source records after digitisation.

Well planned and documented digitisation processes meet all five principles of the *Information Asset Management Policy (GB85/23)*.

2. Scope

This Procedure is applicable to the digitisation of temporary, long-term or permanent value physical information assets, undertaken by the Authority contractors, employees and third parties as a routine administrative process. These *Procedures* do not fully comply with the requirements of GDS 21 (as amended) to allow for the early destruction of hard copy source after digitisation, as the Authority does not have the capacity to maintain digital systems fully compliant with the SRSA *Managing Records in Digital Systems Standard*.

3. Background

Most of the Authority's information assets are now created and received in digital format, however ad hoc hardcopy source records such as invoices and correspondence may continue to be received. Some will have short-term retention periods; others may require permanent retention.

To maximise the efficiency of workflows and access to information assets, digitising the ad hoc physical records may be desirable. Once digitised (scanned) the physical record must be retained and maintained as the Master version. The digital version is an access copy. The Master version (original hard copy) must be filed in the physical file system and retained for the minimum retention period. This process results in a hybrid filing system consisting of digital and physical items. Management, including disposal, must be applied regardless of format, therefore when the Invoices for a specified period have been authorised for destruction, this action is applied to digital and physical items.

4. Procedures

Follow the Digital First principle; ask suppliers to issue invoices, submit reports or correspond in digital formats and only create physical records within the Authority when there is no other reasonable option.

4.1 The following actions should be applied to ad hoc physical records received and created by the Authority.

Appraisal - All information assets must be filed according to the *Information Asset Business Classification, Titling and Filing Procedures* and sentenced according to the relevant GDS as amended, either:

- GDS 40v1 Local Councils and Local Governing Bodies and Authorities (Expiry 31/12/2029)
- GDS 16v1 Native Title Claims (ongoing)
- This process identifies the required retention period (value) of the record and its business classification.

4.2 Digital File Formats - PDF is the preferred file format for all documents. Multi-page documents need to be scanned as a multi-page PDF.

JPG is the preferred format for all access images. Images need to be scanned in full colour as a single page file. Compression is acceptable as the scanned image is the access derivative and does not replace the Master physical image.

4.3 File Titling - All digital files must be titled and saved in the appropriate location. Retaining the automatically applied file title is not acceptable for access or management of information assets. Follow the *Information Asset Business Classification, Titling and Filing Procedures* to ensure consistency, maximising efficiency of retrieval and management.

4.4 Filing the physical item – once digitised, the physical item needs to be filed in the physical file system (a box) after adding the digital file location in pencil (ink marking is not permitted on permanent value items). Due to the size and context of the Authority and the small quantity and range of information assets, unique identifiers are not allocated. Instead, the file path to the digital version is applied. For example, the file path for an invoice or correspondence might be:

GRFMA>Finance>Invoices 2024>[yyyy.mm.dd]

GRFMA>Administration>Correspondence>{yyyy.mm.dd] [ABC Sender]

4.5 Destruction - Once the information asset is eligible and authorised for destruction, all formats, digital and physical, are to be destroyed securely and permanently with a certificate of destruction obtained and saved for long term retention.

Information Asset Disposal Procedures

1. Introduction

This Procedure covers the **disposal** of the Authority's information assets in accordance with the State Records Act and the Authority's *Information Asset Management Policy (GB85/23).* Disposal includes permanent, confidential destruction of temporary records, transfer to other South Australian government agencies as required, and transfer for permanent retention to SRSA.

This Procedure ensures **disposal** programs are conducted lawfully and efficiently and ensures the permanent retention of information assets of importance to the Authority and the State. **Disposal** programs benefit business operations, reduce costs and support compliance with regulatory requirements including the *Local Government Act 1999*, the *State Records Act 1997 and Information Privacy Principles.*

Well planned and documented **disposal** processes meet all five principles of the *Information Asset Management Policy (GB85/23).*

2. Scope

This Procedure is applicable to the **disposal** of the Authority's information assets of temporary, long-term or permanent value, by staff and third parties. This procedure applies to the disposal of information assets in all formats including the permanent deletion of digital data such as electronic files and database entry records, regardless of storage location.

3. Background

Disposal programs include processes associated with implementing records destruction or transfer decisions which have been documented and authorised by the relevant, current SRSA **disposal** schedule.

Lawful **disposal** of information assets includes:

a) Authorised destruction conducted confidentially and permanently
b) Transferring custody to SRSA for permanent retention
c) Storage at an Approved Service Provider (ASP)
d) Transferring ownership to another SA Government agency
e) Migrating information from one system or platform to another

Adherence to the State Records Act, Standards and the Authority's *Information Asset Management Policy* along with application of these *Procedures* ensures information assets are managed and monitored to minimise risk of loss due to:

a) Environmental hazards (e.g. flood or fire) resulting in permanent damage or loss

b) ICT infrastructure failure or compromise (e.g. hacking, viruses) that delete or corrupt digital information assets
c) Use of legacy or bespoke software that is not capable of enabling comprehensive or accurate migration of data to a replacement system
d) Storage on media that is damaged or obsolete, e.g.:
    i. Degraded magnetic media
    ii. Media for which hardware is no longer available
    iii. Software that is no longer usable
e) Staff practices not meeting the Authority's *Information Asset Management Policy* and the following procedures, resulting in:
    i. Destruction of information due to deliberate or accidental action, lack of knowledge or unlawful **disposal** (including destruction without authorisation, abandonment, transfer to a non-government entity and selling).
    ii. Lack of accountability trails for **disposal** decisions.
    iii. Incomplete destruction resulting in remaining information assets being accessible and / or discoverable.
    iv. Taking information assets offsite without authorisation or transferring them to non-government entities.

Implementation of the following procedures ensure that the **disposal** of information assets is:

1. Authorised
2. Underpinned by appraisal
3. Managed
4. Complete and secure
5. Accountable

4. Procedures

The following procedures address the above criteria, through the compilation of well-documented **disposal** activities conducted in accordance with an SRSA authorised **GDS** and Standards.

4.1 **Disposal** Program

5.1.1 Annual review of this *Procedure* and related documents, and whenever business changes.
5.1.2 Continuous sentencing as information assets are processed and entered into a system.
5.1.3 Annual destruction of eligible records including those stored in Cloud based software.
5.1.4 Routine transfer of eligible records to SRSA for permanent retention.

4.2 Appraisal

All information assets must be sentenced according to the relevant GDS as amended, either:

GDS 40v1 Local Councils and Local Governing Bodies and Authorities (Expiry 31/12/2029)
GDS 21v5 Disposal of Hardcopy Source Records after Digitisation (expiry 31/12/2028)
GDS 16v1 Native Title Claims (ongoing)

4.3 Destruction of temporary retention information assets

4.3.1 Register – Prior to authorising destruction, all items must be entered into the *Information Asset Control Register* (Excel Workbook) and sentenced according to GDS 40, 21 and 16 as amended and approved by SRSA. This process provides intellectual control by providing the following details for each item:

a) Physical or digital location
b) Title and description sufficient to indicate the purpose, content and context:
    i. Function / Activity in accordance with the Business Classification Scheme
    ii. Start and End dates, with the end date being the date of last action, completion or expiry
    iii. Applicable GDS, class and retention period
    iv. Action date to indicate when the item becomes eligible for review, destruction or transfer to SRSA.

4.3.2. Review - Once items are eligible for destruction, sentencing must be reviewed for any changes in business or legislative requirements including amendments to the applicable GDS, which may have occurred since sentencing.

4.3.3. Authorise - After review, a consignment list of items eligible for destruction must be created and inserted into an *Information Asset Disposal Authorisation Form.* Destruction is authorised once all required parties have reviewed the consignment list and signed the form to authorise destruction. Parties include the:

a) Sentencer
b) Executive Officer (EO)

4.3.4. Destroy - Secure and confidential destruction must be undertaken by a third-party provider within 60 days and a Certificate of Destruction obtained. *Note: The same process applies to the permanent destruction of data in digital business systems.

4.3.5. Evidence - The records documenting this process, including the completed *Information Asset Disposal Authorisation Form* and *Certificate of Destruction* are to be managed and maintained according to GDS 40 minimum requirements and for as long as needed. Add the destruction Date and Destruction Certificate details to the 'Destroyed' sheet in the *Information Asset Control Register* (Excel Workbook).

4.4 Transfer of Custody to SRSA

4.4.1 Register - all items must be entered into the *Information Asset Control Register* (Excel Workbook) and sentenced according to GDS 40, 21 and 16 as amended and approved by SRSA. This process provides intellectual control by providing the following details for each item:

a) Physical location
b) Title and description sufficient to indicate the purpose, content and context
c) Start and end dates, with the end date being the date of last action or expiry
d) Applicable GDS, class and retention period
e) Action date to indicate when the item becomes eligible for destruction

4.4.2 Review - Once items are eligible for transfer, sentencing must be reviewed for any changes in business or legislative requirements including amendments to the applicable GDS, which may have occurred since sentencing.

4.4.3 Propose – Prepare and submit a Transfer Proposal in accordance with SRSA standards and guidelines. The Proposal must be authorised by the EO. If the Proposal is accepted, a Records Access and Description List (RADL) must be submitted for each series and approved by SRSA before physical transfer can be arranged.

4.4.4 Evidence - The records documenting this process, including the Transfer Proposal, RADL and Receipts, are to be managed and maintained according to GDS 40 minimum requirements and for as long as needed.

4.5 Transfer to Approved Service Provider

5.5.1 Refer to SRSA guideline for *Management and Storage of Temporary Information Assets with an Approved Service Provider.*

4.5.1 Register - all items must be entered into the *Information Asset Control Register* (Excel Workbook) and sentenced according to GDS 16, 21or 40, as amended and approved by SRSA. This process provides intellectual control by providing the following details for each item:

- Physical or digital location
- Title and description sufficient to indicate the purpose, content and context
- Start and end dates, with the end date being the date of last action or expiry
- Applicable GDS, class and retention period
- Action date to indicate when the item becomes eligible for destruction

4.5.2 Permanent records – SRSA must approve the transfer of permanent records that are more than 15 years old and not required for current business purposes, to storage with an ASP, as these are eligible for transfer to SRSA.

4.6 Transfer of ownership

In any instance where information assets are required to be transferred from the Authority to another South Australian Government agency, the relevant SRSA Standards and Guidelines must be followed. This may include the guideline for managing records during *Administrative Change*.

4.7 Migration

The migration, conversion or transfer of information assets from their original digital context must be undertaken by such methods as required to ensure ongoing authenticity, reliability, integrity and usability. Ensuring the process is compliant with the SRSA Standard Managing Digital Records in Systems will include:

a) Planning to ensure data and associated metadata is not lost or corrupted.
b) Documenting to ensure knowledge of the process remains accessible for as long as needed.

Digital Signature Procedures

1. Introduction

This Procedure covers the digital signing of documents created or issued by the Authority.

This Procedure ensures the reliability and authenticity of information assets created and maintained in a digital environment.

2. Scope

This Procedure is applicable to the signing of information assets requiring a signature as evidence of compliance, confirmation or agreement. Digital signatures are currently applied by the Chair of meetings to confirm meeting minutes and by the constituent Councils to declare independence of the external auditor.

3. Background

Most of the Authority's information assets are now created and received in digital format. Applying digital signatures ensures the documents remain in digital format, reducing the need to manage and store hardcopy information assets.

DocuSign, a tool within the Adobe tool collection, is commonly used for secure digital signatures. PDF documents are uploaded to the Adobe online account where names of signers are entered. A link is then sent to the signer(s), allowing the digital signing from various and remote locations without having to print, post or scan. Only an individual's email address should be associated with the named signer as the evidential value of digital signatures relies on only the signer having access to the specified email address. Do not use generic or shared email addresses such as Office@ or Council@ as these are accessed by many users and do not specifically name the individual signing.

4. Procedures

The following procedures ensure that digital information assets requiring a signature for completion are reliable and can be maintained in digital format for as long as needed.

4.1 Prepare, create or save a received .pdf document as a draft in appropriate folder.
4.2 Upload the document to DocuSign. Insert signer(s) and select options as appropriate for the document.
4.3 Review, checking all details are entered as required then Send for signing.
4.4 Once signing is completed, all signers will receive a copy of the fully signed document. Save the final, fully signed .pdf in the appropriate file location.
4.5 The draft document may now be deleted.

3.2 DEFINED RESOURCES, ROLES AND RESPONSIBILITIES

The scope of resources, roles and responsibilities of the Authority and its Executive Officer are defined in the GRFMA Charter and the Executive Officer Service Contract. Financial resources and planning are included in the Strategic Management Pan and Annual Budgets.

The Executive Officer is responsible for implementing the IAM Program and Plan as defined in this *IAM Manual*.

The GRMFA Board is responsible for ensuring adequate resources are available to allow implementation of the IAM Program and Plan. Resources also need to be allocated for:

- annual review and updating of the IAM Manual,
- utilising the Self-Assessment Tool annually,
- actioning one or more Assessment Priorities as identified from the annual Self-Assessment.

3.3 ACCESS AND RELEASE SCHEMES

The Authority proactively releases information to the public in accordance with the SA government Open Data Principle 1. This is achieved through publication of digital information on the GRFMA webpage and transfer of permanent value physical items to SRSA for public access.

The GRFMA webpages are hosted on the Council of Gawler website. Information assets proactively released include:

- Annual Reports
- Strategic and Business Plans
- Financial Statements and Budgets
- Feasibility Reports and Project Reviews
- Meeting Proceedings and Key Outcomes
- Board Member composition
- Policies

Permanent value physical items have been transferred to the custody of SRSA for ongoing preservation and public access. The SRSA *Public Access Determinations* are followed to ensure items are open for public access immediately, or at least as early as possible. The following series have been transferred to SRSA and are open to public access:

- GRS18311 Minute Books, 2002-2014
- GRS18312 Publications (including Annual Reports), 2002-2018
- GRS18313 Board and Committee Proceedings, 1986-2017

3.4 SECURITY CONTROLS

The Authority understands the value of its information assets and therefore the need to ensure they remain secure from accidental loss and leakage (internal) or external threats such as malware[2] and hacking.

External threats are mitigated by ensuring:

- Quality malware protection software is installed on all computers which store the Authority's information assets either for ongoing management or for temporary use (such as Members emails and digital storage).
- All computers and software applications are password protected.
- Passwords are frequently changed and unique for each application and device.
- Two-factor authentication is applied in all instances where available.
- Digital data is stored in Australia (achieved by selecting the M365 option for Advanced Data Residency). While not explicit, this requirement is preferable and implied in the SRSA *Cloud Computing and Records Amanagement Guideline*. Installing the Advanced Data Residency add-on ensures that the Authority's information assets are not subject to the data privacy requirements of any other another country. SRSA advice on Cloud Computing provides additional information in relation to requirements related to compliance with the Information Privacy Principles Instruction (IPPI) (see 3.5 Privacy Protection and Considerations).

Internal threats are mitigated by ensuring:

- All software applications are backed-up so that data can be restored in cases of accidental deletion. M365 provides access to previous versions and deleted data for 30 days.
- Email recipient details are carefully checked before sending, especially when attachments are included, to ensure items are sent to the correct person / email address. Data leakage occurs when sending information assets to the wrong person / email address. This issue is particularly important when sending information to parties external to the Authority.
- Passwords and two-factor authentication details are not shared, and passwords or passphrases are routinely changed.
- All application Administrator details and passwords are changed during Executive Officer handovers.

[2]Malware is any software intentionally designed to cause disruption to a computer, server, client, or computer network, leak private information, gain unauthorized access to information or systems, deprive access to information, or which unknowingly interferes with the user's computer security and privacy. Wikipedia

3.5 PRIVACY PROTECTION AND CONSIDERATIONS

Personal information' is any information about a person where that person can be identified from the information. Personal information includes details such as name, address, date of birth, financial or health status, alleged behaviours and licensing details. Photographs, video footage and sound recordings may also include personal information.

The Authority ensures Privacy Rights surrounding personal information are protected by adopting and implementing the Information Privacy Principles Instruction (IPPI) as documented in Premier and Cabinet Circular 12 – information Privacy Principles Instruction.

3.6 DISPOSAL DETERMINATIONS

Disposal actions include destruction and transfer to SRSA or another SA government agency due to administrative change. Actions are determined in accordance with SRSA authorised disposal schedules. All items are sentenced under *GDS 40 Local Councils and Local Governing Bodies and Authorities*, as amended, prior to review and authorisation for disposal. Sentencing and review includes applying disposal freezes as appropriate. *GDS 16 Native Title Claims*, ongoing, must be considered when sentencing any information assets related to land acquisition or development.

The Authority does not provide care to any persons including children, aged persons, veterans or persons with disabilities, therefore the following disposal freezes are not applied as the Authority's information assets are not of relevance to:

- *GDS 32v2 Records of Relevance to the Royal Commission into Institutional Responses to Child Sexual Abuse* (Expiry 31/12/2024)
- *GDS 36v1 Records of Relevance in Relation to Child Abuse or Alleged Child Abuse* (Expiry 31/12/2024)
- *GDS 37v1 Records of Relevance to the Royal Commission into Aged Care Quality and Safety* (Expiry 31 /12 2025)
- *GDS 38v1 Records of Relevance in Relation to the Royal Commission into Violence, Abuse, Neglect and Exploitation of People with Disability* (Expiry 31 /12 2025)
- *GDS 43v1 Records of Relevance in relation to the Royal Commission into Defence and Veteran Suicide* (Expiry 31/12/2025)

Permanent value physical information assets are transferred to SRSA in accordance with the SRSA *Transfer Standard*. Permanent value digital information assets must be retained and managed, ensuring they remain reliable, authentic, useable and accessible until such time as they can be transferred to a SRSA digital repository. See Information Asset Disposal Procedures for further details.

3.7 COMPLIANT SYSTEMS

The Authority is a micro agency. Executive Officer Services are engaged in accordance with an agreed contract for service. The Authority does not engage any employees, utilise volunteers, or require Board Members to manage information assets. Information assets created or received by Members are submitted to the Executive Officer for management. The information assets requiring management is narrow and confined by the scope of the GRFMA Charter.

Due to the unique nature of the Authority, it has not implemented and EDRMS (Electronic Document and Records Management System) with the capabilities that would enable full and certified compliance with the SRSA *Managing Digital Records in Systems Standard* and *Minimum Recordkeeping Metadata Standard,* allowing for the destruction of hard copy source records after digitisation (GDS 21).

Instead, this *Information Asset Management Manual* detailing the IAM Program and Plan, including Policy and Procedures, has been developed and implemented to ensure risk appropriate compliance with SRSA Standards. 2. Value and Risk Assessment demonstrates low risks associated with 'in place' information assets management; managing information assets within the digital application where they are created and/or managed rather than capturing into a dedicated EDRMS. Information assets managed 'in place' (M365 OneDrive) are listed in section 1. Information Asset Audit.

4. EDUCATION

The Authority recognises the value of information assets, the importance of IAM and the need for awareness training as a minimum requirement. In addition, the Executive Officer must have additional FOI Officer training. IAM consultants are engaged as required for advice or to undertake tasks outside the capabilities of the EO and the scope of this *IAM Manual*.

4.1 Board Members, the Executive Officer, Employees and Volunteers undertake IAM awareness training as part of the induction process, if not previously undertaken. SRSA online module 'An Introduction to Information Management' is used for this purpose. Course content may be modified from time to time.

4.2 The Accredited FOI Officer must have undertaken related Freedom of Information training available from SRSA. The Executive Officer, when not the Accredited FOI Officer, needs to have undertaken the minimal level of FOI General Awareness training. For further information go to SRSA factsheet What is an Accredited FOI Officer?

4.3 Familiarity with and implementation of this *IAM Manual* provides most of the information required to undertake routine, operational IAM. Ensuring this *Manual* is reviewed and updated annually will facilitate ongoing improvements to the Authority's IAM Program through implementation of the Plan, improving behaviours to align with the principles detailed in the IAM Policy.

5. SELF-ASSESSMENT AND REPORTING

The SRSA *Self-Assessment Tool* (Excel Workbook) is utilised to measure IAM maturity annually (July). This Workbook includes four sheets:

- Instructions
- Detailed Assessment
- Capability Model
- Assessment Priorities

The ‘Assessment Priorities’ report generated from the ‘Detailed Assessment’ sheet is used to inform decision making for future improvements. The ‘Capability Model’, also generated from the ‘Detailed Assessment’, provides data for responding to SRSA Maturity Surveys. Surveys are likely to be issued every 3-6 years.

5.1 Create a new version of the *Self-Assessment Tool* each year.

5.2 Follow the ‘Instructions’ to review and update the ‘Maturity and Capability Level’ and ‘Notes’ fields on the ‘Detailed Assessment’ sheet.

5.3 Data automatically populates into the ‘Capability Model’ sheet. Ensure the Authority’s details and version are updated at the top of this sheet.

5.4 Follow the instructions to generate the report on the ‘Assessment Priorities’ sheet.

5.5 Submit the ‘Assessment Priorities’ report to the Audit & Risk Committee for review.

5.6 Ensure that responses to all SRSA Surveys are submitted within the required timeframes.

Appendix A: NAP Guidelines - Destruction of Unofficial Records

What is Normal Administrative Practice (NAP)?

NAP is the concept applied to the routine destruction of material of a transitory, facilitative, ephemeral or non-business nature. NAP is primarily intended to permit disposal of ephemeral records that might technically be official records under the State Records Act definition but that have no ongoing value to agencies and where policies, procedures, knowledge and experience suggest that the document does not need to be saved into a business system.

Destruction is undertaken after applying the NAP test (below) to determine that no information of ongoing value to the Authority will be lost. It applies to the routine destruction of drafts, duplicates and publications, regardless of format, created or received by the Authority.

Authority to use NAP

NAP is provided in the interests of efficient recordkeeping and extends to material of ephemeral and transitory value only. Destruction of the Authority's unofficial information assets according to NAP is authorised by GDS 40 amended.

NAP in digital media

Recordkeeping and NAP principles apply to all formats including:

- voice mail,
- e-mail,
- facsimiles,
- word processed documents, spreadsheets, etc.

The NAP test

Where the information is not duplicated in the Authority's business system, ask:

• Does the material form part of an Authority transaction?

• Does it add value to an existing record?

• Does it show how a transaction was dealt with?

• Does it show how a decision was made?

• Does it show when or where an event happened?

• Does it indicate who was involved or what advice was given?

• Is it a formal draft of a Cabinet submission, an agreement or a legal document?

• Is the material included in the current GDS 40 or relevant to a disposal freeze?

If the answer to any of these questions is YES, then the material must not be destroyed according to NAP. File the item according to IAM procedures.

Examples of material that may be eligible for destruction under NAP

Only material or data included in the five categories outlined below may be deleted or destroyed securely and confidentially from business systems according to NAP. Disposal of any other records, physical or digital, must be undertaken in accordance with current disposal schedules.

	Category	Examples	Notes
1.	transitory or short-term items including electronic data	• phone messages, notes, compliment slips, • messages and notes, required for only a few hours or a few days, • information received including copies of office notices and circulars.	Includes voice-mail, email and facsimiles not required for ongoing Authority business evidence. Disposal of master notices, circulars and distribution records must be undertaken in accordance with a current, applicable GDS.
2.	rough working papers and/or calculations created in the preparation of official records and drafts not intended for further use or reference,	• rough notes not intended for further use, • word processing documents and spreadsheets in electronic format after updating (excluding official version drafts of agreements, submissions and legal documents), printing, or transfer to electronic recordkeeping systems	Some record classes cover the disposal of working papers. Rough working papers could be defined as pre first draft notes/calculations/outlines. Disposal of official drafts must be undertaken in accordance with a current, applicable GDS.
3.	duplicate copies of material retained for reference purposes only	• Superseded or distributed copies of instructions, guidelines, standards, etc., • extra copies of records no longer required for reference purposes, • copies of Authority material/records created for reference/ease of access.	To avoid confusion, always stamp or title as COPY to enable easy identification and NAP destruction. Disposal of master records must be undertaken in accordance with a current, applicable GDS.
4.	published material received or collected which does not form an integral part of an Authority record	• brochures, catalogues, price lists, unsolicited promotional material, etc. received from external sources, • copies of Legislation, regulations, standards etc., • copies of published items kept for personal reference.	For records of Authority input into the development or review of legislation, regulations etc. See GDS 30v2:13.13 for retention and disposal requirements.
5.	system printouts that are not part of regular reporting procedures and not required for ongoing use	• system log reports to verify or monitor data on an ad hoc basis, • printouts used to answer ad hoc queries, • copies printed for proofreading.	Printouts generated from routine reporting, including bona fide leave reports, must be disposed in accordance with GDS 30v2: 13.22.5

Appendix B: Business Classification Scheme

Business Classification Scheme	Code	GDS 40 Class	Retention Period
Board and Committee	**1.0**		
Board Meetings	1.1	3.1	Permanent
Audit & Risk Committee	1.2	3.1	Permanent
Technical Assessment Panel	1.3	3.1	Permanent
Publications	**2.0**		
Annual Reports	2.1	5.3	Permanent
Other Publications	2.2	100.6	Permanent
Infrastructure Management	**3.0**		
Inspections	3.1	82.7 (design / construction) and 82.13 (inspections / maintenance)	Indefinite - Retain 6 yrs. after asset disposal. (Permanent items captured in 1.0 Board and Committee)
Maintenance	3.2		
Plans	3.3		
Reports	3.4		
Finance	**4.0**		
(Sub Folders are arranged by Year)		6.3, 6.5, 6.7, 6.8, 6.9	Temporary (6 years)
Strategic Management	**5.0**		
Annual Business Plan	5.1	5.10 and 5.14	Temporary (6 years)
Long Term Financial Plan	5.2	5.10 and 5.14	Temporary (6 years)
Strategic Management Plan	5.3	5.10 and 5.14	Temporary (6 years)
Asset Management Plan	5.4	5.10 and 5.14	Temporary (6 years)
Admin	**6.0**		
Member Management	6.1	2.4	Temporary (6 years after exit)
(Subject Folders as required, arranged alphabetically)		Various routine administrative operations	Temporary (6 years) (Permanent items captured in Board or Committee agendas)
Information Asset Management	**7.0**		
Manual	7.1	66.9	Temporary (20 years)
Assessments	7.2	66.13	Temporary (6 years)
Destruction	7.3	66.14	Temporary (50 years)
Transfers	7.4	66.11	Indefinite
Reports	7.5	104.1	Temporary (6 yrs.)

Appendix C: Risk Assessment Matrix

The Risk Assessment Matrix identifies the risks associated with the Authority's non-compliance with internal and external requirements to create, retain and manage information assets.

The risk likelihood against the risk consequence determines the overall risk rating.

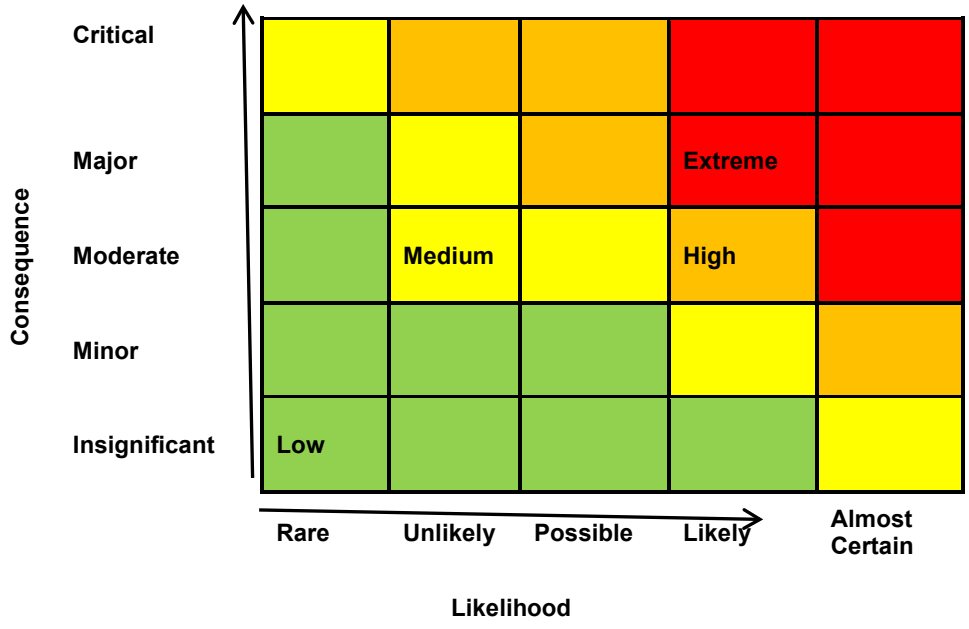
1. Overall Risk Rating

Extreme Risk	Immediate action required along with senior management commitment
High Risk	Senior management attention required, and development of an action plan
Medium Risk	Management responsibility must be specified (i.e. accountability defined)
Low Risk	Manage by routine procedures

2. Risk Likelihood

Almost certain	The event is expected to occur within the next 12 months
Likely	The event is more likely than not to occur within the next 12 months
Possible	The event may occur within the next 12 months
Unlikely	The event is not likely to occur in the next 12 months
Rare	The event will only occur in exceptional circumstances

3. Risk Matrix



4. Risk Consequence

	Financial	Stakeholders	People	Product / Service delivery	Compliance / Legal
Critical	• Financial loss greater than $1 million (operating budget). • Financial loss greater than $2 million (insurance reserves).	• Substantial long-term damage to brand and degradation of public perception of the Authority, affecting whole business. • Significant state-wide negative publicity, i.e. from TV and newspapers for more than one week. • the Authority subjected to state parliamentary enquiry.	• Death due to negligence. • Inability of the Contractor to have available adequate resources (such as personnel to work, finance to provide the services • Dismissal of the Board and/or the EO.	• Loss of any service delivery or business operations for more than 4 weeks.	• Significant legal, regulatory or internal policy failure. • Regulatory sanctions. • Class action against the Authority.
Major	• Financial loss greater than $500k and less than $1 million (operating budget). • Financial loss greater than $1 million and less than $2 million (insurance reserves).	• Long term damage to brand and degradation of public perception of the Authority, affecting whole of business. • Significant state-wide negative publicity, i.e. from TV and newspapers for up to one week. • Questions raised about the Authority in state parliament.	• Serious injury. • Dangerous near miss. • Inability of the Contractor to have available adequate resources (such as personnel to work, finance to provide the services • Dismissal of a Board member or EO	• Loss of any service delivery or business operations for more than 5 days.	• Major legal, regulatory or internal policy failure. • Regulatory fines. • Multiple litigation cases against the Authority.

	Financial	Stakeholders	People	Product / Service delivery	Compliance / Legal
		• High impact/long term issue requiring Board intervention.			
Moderate	• Financial loss greater than $100k and less than $500k (operating budget). • Financial loss greater than $500k and less than $1 million (insurance reserves).	• Moderate term damage to brand and degradation of public perception of the Authority, affecting key areas of the business. • Minor state-wide negative publicity, although manageable through good public relations. • the Authority under scrutiny from the Treasurer. • High impact requiring Executive Officer intervention or Board notification.	• Lost time due to workplace injury. • Inability of EO services to attend the business for more than 2 weeks. • Unexpected / unplanned resignation or dismissal of a key senior staff members.	• Loss of any service delivery for greater than 3 days.	• Moderate legal, regulatory or internal policy failure. • Regulatory investigation. • Individual litigation taken against the Authority.
Minor	• Financial loss greater than $10k and less than $100k (operating budget). • Financial loss greater than $50k and less	• Short term damage to brand and degradation of public perception of the Authority, affecting key areas of the business. • Incident requiring management intervention.	• Minor workplace injury – no lost time. • Inability of EO services to attend the business for more than 1 week.	• Loss of any service delivery or business operations of 1 day.	• Minor legal, regulatory or internal policy failure. • Regulatory attention.

	Financial	Stakeholders	People	Product / Service delivery	Compliance / Legal
	than $250k (insurance reserves).				
Insignificant	• Financial loss less than $10k (operating budget). • Financial loss less than $50k (insurance reserves).	• Issue of limited impact. • Minor brand damage and degradation of public perception of the Authority's values i.e. trust, affecting areas of the business.	• Unplanned resignation or dismissal of a small number of staff members. (Nil Employees)	• Loss of any service delivery or business operations less than 1 day.	• Insignificant legal, regulatory or internal policy failure.

Appendix D: Disposal Authorisation Proforma

GRFMA

Expired Records

Disposal Report - Review and Authorisation

Disposal Type	[Destruction / Transfer]

Disposal Authority	GDS 40v1
Disposal Freezes	GDS 32 Not Applicable GDS 16 – Reviewed

Date Authorisation Form Compiled	[DD/MM/YYYY]
Records Date Range	[DD/MM/YYYY to DD/MM/YYYY]
Latest Expiry Date	[DD Month YYYY]
Number of Listed Items	[# items]
Sentenced by	[Company, Name]
Sentencer Signature	
Signed Date	

Disposal Authorised by	EO: [Name]
Authorised Signature	
Authorisation Date	

Disposal Process	[Method - Certified]
Disposal Authorisation No.	[GRFMA-DA-YYYY]

Box No.	Title / Description	Start Date	End Date	Disposal Class	Yrs	Action Date	Comments