NCSS
National Council
of Social Service

DATA MANAGEMENT GUIDE

National Council of Social Service

2021

TABLE OF CONTENTS

KEY AIMS AND SCOPE

The Data Management Guide

aims to provide guidance to Social Service Agencies (SSAs) and Charities (hereinafter referred to as "Agencies") on recommended practices for handling data in a data lifecycle approach, with relevant resources, guides and references.

Benefits of using the Data Management Guide

- Adopt a lifecycle approach to data management when handling and managing data.
- Identify critical data protection and cybersecurity procedures that should be implemented throughout the lifecycle.
- Conduct a review of the present data management practices, reflect on them and identify shortcomings.

Who is this Guide for?

Individuals (or part of a team) who:

- Oversee and/or develop agency practices and standards for handling data; and
- Oversee transfer of data between teams and across agencies.

How to use the Guide?

This guide is organised along five stages of the data management lifecycle. There are checklists and resources highlighted in each lifecycle stage as well as key support available that agencies can tap on for assistance.

☑ Checklists for self-evaluation

Additional resources for better understanding

Note: Agencies can attend the e-learning progamme on Personal Data Protection Act (PDPA) to learn and understand key terms and obligations under the PDPA.SSAs that wish to carry out a self-assessment of their personal data protection policies and practices can do so via the PDPA Assessment Tool for Organisations (PATO).

IMPORTANCE OF EFECTIVE DATA MANAGEMENT

What is Data Management?

End-to-end data management is the practice of collecting, storing, using, sharing and archiving/destroying data in a secured and efficient manner.

Why do you need data?

Data contributes to knowledge building; good data helps agencies in their evidence-based decision-making process to:

- Enhance and sustain continuity of care for service users
- Measure impact of service offerings
- Identify trends and gain actionable insights on service users' needs
- Enhance service planning, operations and quality of existing services
- Optimise resources or improve efficiencies

Key reasons why effective data management is important for agencies:

1 Minimise potential errors and risks by establishing data handling processes and policies.

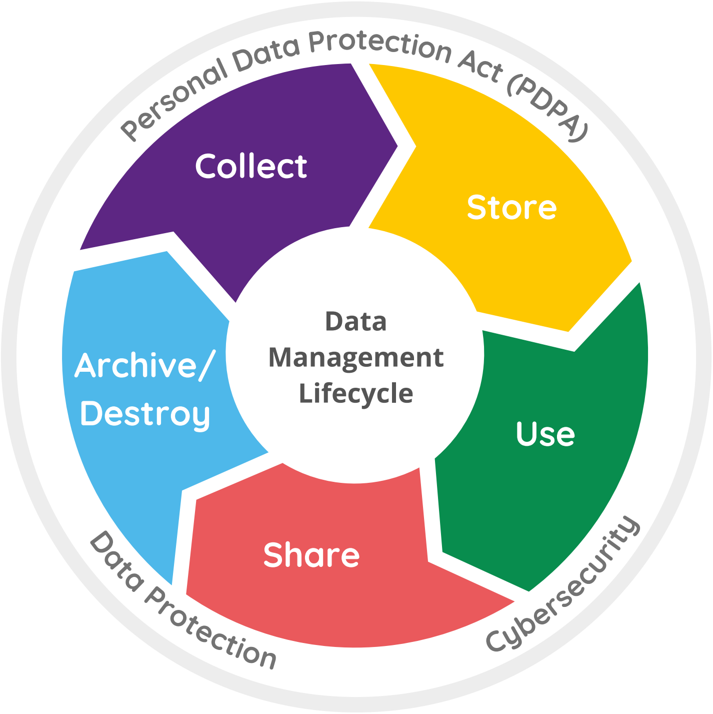
2 Uphold service users' trust in handling their sensitive information by complying with legislative standards.

3 Optimise data for agency's needs (e.g. to identify trends for service planning, enhance quality of service delivery, monitor service users' journeys etc.).

DATA MANAGEMENT GUIDE LAYOUT

As part of the digital transformation journey, agencies will be presented with new opportunities to refine, leverage and capitalise on existing and new data to achieve organisation excellence.This Data Management Guide, while non-exhaustive, supports and guides agencies in handling data in a typical lifecycle approach and to build its data management capability.

The Guide is organised along five stages of the data management lifecycle.



01 About the Data Management Guide

CHAPTER 1: COLLECT DATA

- Establish a Primary Purpose for Data Collection
- Understand the Different Types of Data
- Understand Ways to Collect Data
- Clean and Classify Data Collected
- Understand Personal Data Protection Act (PDPA) Obligations in Data Collection

CHAPTER 2: STORE DATA

- Understand the Advantages of Storing Data on Cloud
- Choose a Suitable Cloud Service Provider (CSP)
- Understand Ways to Protect Stored Data
- Understand Personal Data Protection Act (PDPA) Obligations in Data Storage

CHAPTER 3: USE DATA

- Verify Purpose for Data Usage
- Understand Ways to Use Data
- Establish Internal Protocols and Procedures for Data Usage
- Understand Personal Data Protection Act (PDPA) Obligations in Data Usage

CHAPTER 4: SHARE DATA

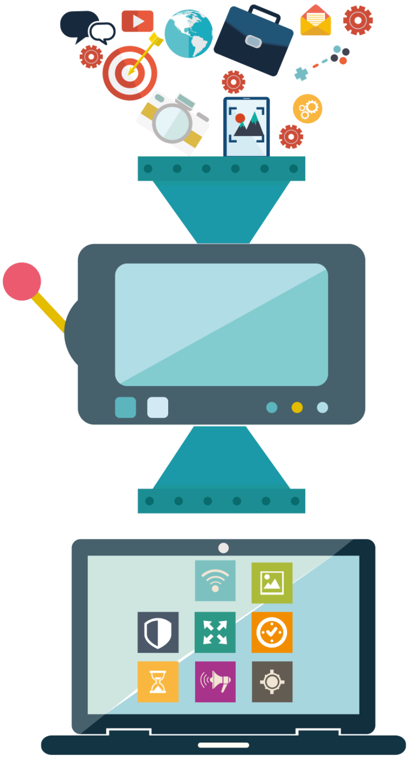
- Develop a Purpose for Data Sharing
- Establish a Data Sharing Agreement (DSA)
- Assess Data for Sharing
- Understand Ways to Share Data
- Understand Personal Data Protection Act (PDPA) Obligations in Data Sharing

CHAPTER 5: ARCHIVE/DESTROY DATA

- Understand the Benefits of Archiving Data
- Assess Data for Archival vis-à-vis Destruction
- Archive and Destroy Data in a Secured Manner
- Understand Personal Data Protection Act (PDPA) Obligations in Data Archival and Destruction

Note: While some references within the guide may point to private organisations' websites as the reference points are intended for as further reading and do not constitute as endorsement by NCSS on any associated products, vendors or points of views.

CHAPTER 1: COLLECT DATA



CHAPTER 1: COLLECT DATA

Data collected can be used to analyse and derive insights for organisational needs. Data - quantitative and qualitative - can be obtained electronically in multiple formats (e.g. excel spreadsheets, pictures, recordings) and/or non-electronically (e.g. manual forms).

Overview

Focus on collecting data from various sources

- Establish a Primary Purpose for Data Collection
- Understand the Different Types of Data
- Understand Ways to Collect Data
- Clean and Classify Data Collected
- Understand Personal Data Protection Act (PDPA) Obligations in Data Collection

Checklists

Help your agency meet minimal baselines

- Key Components of Data Quality
- Data Cleaning Techniques
- PDPA Obligations to Highlight when Collecting Personal Data

Resources

Apprise on other guidelines and support related to data collection

Your agency should adopt the concepts in this guide, along with the following resources:

- Personal Data Protection Policy Development and Communication
- Personal Data Protection Notice Generator
- Data Inventory Map
- Appointment of a Data Protection Officer

Chapter 1, Section (A)

Establish a Primary Purpose for Data Collection

An established primary purpose for data collection will help your agency to:

1. Determine the type of data required for collection.
2. Identify sources and methods to collect required data.
3. Plan how you can draw actionable insights from the data.

Data Collection Purposes	Potential Data Required
Establish service required by users	• Users' profile • Users' needs
Measure impact of service offerings	• Programme outcomes
Identify trends and gain actionable insights on service users' needs	• Customer feedback - survey data, call centre notes • Customer behaviour – website or mobile app usage, transaction history • Performance data – conversion, engagement, bounce rates
Enhance service planning, operations and quality of existing services	• Client records • Case notes

Chapter 1, Section (A)

Agencies should ensure that information collected is relevant for the data collection purpose. Here are some good data collection practice and resources:

01 PERSONAL DATA PROTECTION ACT (PDPA)

Refer to Chapter 1, Section (E) to understand PDPA obligations in data collection.

02 YOUR AGENCY'S INTERNAL DATA POLICIES[1]

Internal data policies should document the agency's data management standards and the Do's and Don'ts when managing data. The policies should be reviewed regularly to ensure its relevance and new policies should be approved by the management.

Personal Data Protection Policy Development and Communication

As part of corporate governance, it is recommended to develop and communicate a Personal Data Protection Policy to both your internal (e.g. staff) and external stakeholders (e.g. service users). This will:

- Provide clarity to internal stakeholders on the responsibilities and processes on handling personal data in their day-to-day work.
- Demonstrate accountability to external stakeholders by informing them on the ways in which your agency handles personal data.

Your agency can also consider developing internal policies dedicated to specific areas that require elaboration. For considerations in developing data protection policy, refer to Part II: What Should Be in a Policy? of Guide to Developing a Data Protection Management Programme.

[1] This includes the Personal Data Protection Policy. To demonstrate accountability, useful initiatives include making your agency's Personal Data Protection Policy available on website or providing the data protection policy promptly when requested by stakeholders.

Chapter 1, Section (A)

Personal Data Protection Notice Generator

Your agency can utilise the Personal Data Protection Notice Generator, a free-to-use tool, to generate basic data protection template notices to inform your stakeholders such as staff, service users and volunteers etc on how you manage personal data.

Chapter 1, Section (B)

Understand the Different Types of Data

Common types of data collected by agencies within the sector include:

Types of Data	Examples
Personal Data Data about an individual[2] who can be identified from that data, or, from that data and other information to which your agency has or is likely to have access	• NRIC number • Mobile contact • Financial and family situation • Medical history
Case Data Information collected by social service professionals through their interactions with service users, and actions taken to address their prevailing service needs	• Case notes • Referral agencies • Interventions
Programme Data Data in relation to the programme[3]	• Programme's key performance indicators (KPIs) • Funding and disbursement amounts • Milestone achievements • User feedback

[2] Individuals are not limited to service users only, but include professionals, donors and agencies' staff etc whose personal data can be found in case, programme, system and research data.

[3] For services and programmes funded by the Ministry of Social and Family Development (MSF)), agencies are required to store the relevant data in the Social Service Net (SSNet); an integrated case management system developed by MSF for the social service sector.

Chapter 1, Section (B)

Types of Data	Examples
System Data Data and information generated, uploaded, downloaded, received, processed or otherwise collected by the system in connection with the user's use of the system	• Hardware performance data • Software performance data • Log data capturing time specific events
Research Data Data used to validate original research findings	• Observational data which is captured through observation of a behaviour or activity • Derived/compiled data which is new data created through arithmetic formula or aggregation using data points

Having established the purpose, data type, and requirement, agencies should assess whether existing data is residing within the agency before obtaining the data from relevant stakeholders.

Data Inventory Map

Your agency can utilise a Data Inventory Map to document data handled to understand the lifecycle of data in your agency. Having a Data Inventory Map can also help your agency keep track of data flows within your agency. Your agency should seek to maintain and update the map regularly as part of risk management. Refer to Part III: Risk Identification and Mapping of Guide to Developing a Data Protection Management Programme and Sample Personal Data Inventory Map Template for more information on data inventory maps or data flow diagrams that your agency can adopt.

Chapter 1, Section (C)

Understand Ways to Collect Data

Agencies should consider the different data collection methods and choose the ones that are most cost-effective and are able to meet the agency's needs. If not, data collected that does not meet the established objectives may end up incurring costs to store.

Choosing the right data collection method can make a difference between deriving actionable insights, optimising resources, or resource wastage.

	Quantitative Data	**Qualitative Data**
Broad Data Type	Measurable in nature and can be expressed in numbers or figures.	Descriptive in nature rather than numerical; usually not easily measurable
What does the data serve to answer?	Questions such as 'who?', 'when?', 'where?', 'what?' and 'how many?'.	Questions such as 'why?' and 'how?'.
What are examples of data collection methods?	• Surveys • Questionnaires • Observations • Contextual inquiries	• Interviews • Focus groups • Records and documents

Each method has its advantages and disadvantages which should be thoroughly weighed during data collection, including effectiveness and compliancy of the process.

Chapter 1, Section (D)

Clean and Classify Data Collected

After collecting the data, your agency must take steps to check for data quality, clean, classify, and assign access rights before it enters the agency's database:

1. Step 1: Verify Data Quality
2. Step 2: Clean Data
3. Step 3: Classify Data
4. Step 4: Assign Access Rights

Chapter 1, Section (D)

Step 1: Verify Data Quality

This step will allow your agency to identify data discrepancies upfront and rectify them by taking immediate actions to run checks across multiple data sets, different systems, latest or at-source data (e.g. directly with service users, or, National Digital Identity (NDI) platforms such as MyInfo for personal information validity).

Key Components of Data Quality

Data Quality Components	Checklist	Examples
Validity Degree to which data conforms to defined business rules or constraints	**Mandatory Data Fields** Ensure no missing inputs for mandatory data fields.	'Name' and 'contact number' should not be blank if user's contact details were intended to be collected
	Cross-field Examination Perform cross checks if there are conditions that affect multiple data fields	User's date of discharge from the hospital should not be earlier than admission date
	Unique Requirements Check for unique restrictions, if any	Different service users should not share the same NRIC numbers
	Constrains Ensure data is within its restricted set, if any	Not more than 12 months in a year – Jan, Feb, Mar etc
	Regular Patterns Ensure data follows a specific format, if any. Data not in the required format is deemed to be invalid	• Email addresses should be in the format 'xxx@xxx.com' • Contact numbers should be 8 digits
Accuracy Degree to which data is close to the true values	Check that data is accurate	Contact number 00001234 is not accurate even though it follows a specific 8-digit number format

Chapter 1, Section (D)

Data Quality Components	Checklist	Examples
Completeness Degree to which all required data is known	Check that data is complete and has no missing inputs[4]	Seniors who do not use email communication will not be able to provide email addresses
Consistency Degree to which data is consistent within the same dataset and/or across multiple data sets	Check that data is consistent	Counter-check user's inputs on age (31) through difference in year of data collection (2021) and birth year (1990)
Uniformity Degree to which data is specified using the same unit of measure	Check that data is using the same unit of measure[5]	• Second(s) for time • Kilogram(s) for mass

[4] Challenging to achieve completeness especially if service users are unable to furnish the required information.

[5] Uniformed data is beneficial if data collected is to be merged with existing information in your agency's databases.

Chapter 1, Section (D)

Step 2: Clean Data

This step will allow your agency to fix or remove incorrect, corrupted, incorrectly formatted, duplicates, or incomplete data within a dataset.

Data Cleaning Techniques

Remove Irrelevant Values
Deleted values can be costly to re-obtain. Before deleting, ensure your agency does not need the information.

Remove Duplicate Values
Duplicate values can be caused by service users filling up the same online form twice, system errors, etc. Ensure that they are indeed duplicate values before removing them as it can be costly to re-obtain them.

Take Care of Missing Values
Account for missing values by indicating ‘0’ and ‘missing/NA’ for numerical and categorical values, respectively, if these values cannot be obtained.

While there are many resources available online on data cleaning techniques, some may require data cleaning or visualisation tools especially for larger datasets.

Chapter 1, Section (D)

Step 3: Classify Data

This step will allow your agency to classify the collected data based on its level of sensitivity, value and criticality to the agency should the data be disclosed, altered, or destroyed without authorisation. A risk-based approach to data classification can better ensure the data is managed through appropriate security measures. The data classification process should be well documented in agency's internal data policy.

An example of a typical 3-tier classification for data is as follows:

Data Classification	**Internal-Sensitive**	**Internal-General**	**External**
Impact in event of Data Leakage	Causes serious damage (financial, legal, regulatory, and reputational etc) to agency or sustained emotional injury to individuals	Causes agency to suffer from short-term reputational embarrassment, but do not result in severe non-compliance repercussions	Causes little or no damage to agency or individuals
Level of Access Controls to be Applied	Risk-based and most stringent level of access controls	Risk-based and reasonable level of access controls	Some level of access controls to prevent unauthorised modification or destruction of data
Accessibility/ Use of Data	Limited on a need-to-know basis	Internally accessible to staff; not for public disclosure	Available in public domains, created for public knowledge
Examples	Personal data e.g. medical history and financial details Donors' information including donation quantum	Internal memos or other communications	Agencies' Annual Reports Governance Evaluation Checklists Anonymised data which cannot be used to identify individuals

Chapter 1, Section (D)

Step 4: Assign Access Rights

This step will help your agency reduce security risk by limiting access to the data. This can be done by system administrators via assignment of access rights after having determined the role of the users. Your agency should:

- Re-evaluate your data classification model and assignment of access rights on a periodic basis to ensure they are still appropriate based on changes to legal obligations, use of the data or its value to the agency.
- Establish internal data management policies, standards, and procedures and review them regularly to ensure they adapt to changes in organisational practices and/or legal obligations.
- Establish clear password and lock protocols for sensitive data access where systems access rights assignment is not available.

Chapter 1, Section (E)

Understand Personal Data Protection Act Obligations in Data Collection

The Personal Data Protection Act (PDPA) governs the collection, use and disclosure of personal data by agencies in a manner that recognises both the right of individuals to protect their personal data and the need of agencies to collect, use or disclose personal data for purposes that a reasonable person would consider appropriate in the circumstances.

> "Personal data" means data, whether true or not, about an individual who can be identified –
>
> (a) From that data; or
>
> (b) From that data and other information to which the organisation has or is likely to have access.

PDPA Obligations to Highlight when Collecting Personal Data

Key things to note when collecting personal data:

PDPA Obligations	How can your agency comply with the PDPA obligations?
Consent Obligation	• Seek consent (expressed, verbal, implied or deemed etc.) from the individual for collecting their personal data for the identified primary purpose(s). • Check for exceptions to Consent Obligation. • Inform the individual concerned, should he withdraw his consent, of the likely consequences of withdrawing his consent and proceed to facilitate the withdrawal.

Chapter 1, Section (E)

PDPA Obligations	How can your agency comply with the PDPA obligations?
Purpose Limitation Obligation	• Ensure that the collection, use or disclosure of data by your agency is limited to purposes that are reasonable and/or purposes that the individual has been informed of by the organisation.
Notification Obligation	• Inform individual of the purpose(s) for which their personal data will be collected, used, or disclosed. • Ensure that the underlying objectives or reasons for collecting the data are clearly articulated to the individual at the onset.
Accuracy Obligation	• Ensure that personal data is always accurate and complete e.g. verified against authorised documents, constantly kept up to date by checking with individuals etc.
Protection Obligation	• Classify personal data as 'Internal-Sensitive' (Confidential).
Accountability Obligation	• Publish Personal Data Protection Policy, informing of the personal data that your agency collects and how they will be protected and used.

Appointment of a Data Protection Officer (DPO)

Under the PDPA, your agency is required to designate at least one individual as the Data Protection Officer (DPO) to oversee data protection responsibilities and ensure compliance with the PDPA. The DPO function may be a dedicated responsibility or added to an existing role in the organisation. The appointed DPO may also delegate certain responsibilities to other officers.

CHAPTER 2: STORE DATA

CHAPTER 2: STORE DATA

A large part of storing data involves keeping the data safe. Cybersecurity is the practice of protecting critical systems and sensitive information from digital[6] attacks , regardless of whether data is at rest (in storage), in motion (travels to, from and within cloud) or in use (during processing).

Your agency can refer to the Cybersecurity Essentials for Social Service Agencies and Charities, launched by NCSS, for basic cybersecurity measures that can be adopted to ensure the security and integrity of your agency's IT assets, systems, and users' data.

Overview

Focus on good cybersecurity and data protection practices in storing data on cloud servers i.e. when data is at rest

- Understand the Advantages of Storing Data on Cloud
- Choose a Suitable Cloud Service Provider (CSP)
- Understand Ways to Protect Stored Data
- Understand Personal Data Protection Act (PDPA) Obligations in Data Storage

Checklists

Help your agency meet minimal baselines

- Considerations for Choosing a Cloud Service Provider (CSP)
- Cyber Incident Response and Reporting
- PDPA Obligations to Highlight when Storing Personal Data

[6] More details on cybersecurity can be found here: https://www.ibm.com/topics/cybersecurity.

CHAPTER 2: STORE DATA

Resources

Apprise on other guidelines and support related to data storage

Your agency should adopt the concepts in this guide, along with the following resources:

- Considerations when using Cloud Services to Process Personal Data
- Good and Enhanced Practices of Cloud Computing
- Good and Enhanced Practices of End-to-End Security
- Systems-in-built Mechanisms to Protect Data Integrity
- Factors for Consideration in Establishing Data Backup Policy
- Continuing Education and Training (CET) Programmes in Cybersecurity (funded by SkillsFuture Singapore (SSG))
- Data Protection and Cybersecurity Consultancy Grant
- Data Protection Trustmark (DPTM)

Chapter 2, Section (A)

Understand the Advantages of Storing Data on Cloud

Your agency can benefit from storing data on cloud in the following ways:

01

GREATER MOBILITY

Data can be accessed remotely. Your agency need not develop and/or manage onsite IT resources.

02

GREATER EFFICIENCY

Cloud service providers (CSPs) account for maintenance, up-to-date software, security and support of cloud. Your agency can free up IT resources to focus on organisational needs/goals.

03

GREATER SCALABILITY

Cloud servers can better meet dynamic demands via the CSP or add-on features. Your agency need not undergo complex updates to your IT infrastructure.

Note: It is useful to have a balanced understanding of pros and cons, so that your agency can be more prepared to mitigate any associated risks. Given that security baselines vary across CSPs, your agency should exercise due diligence in choosing your cloud service providers (CSP). Refer to Chapter 2, Section (B) for considerations when choosing a suitable CSP.

If your agency's data is currently hosted on-premise servers and you are considering to transit to cloud servers, you can compare the key differences and similarities between cloud and on-premise servers to make an informed decision.

Chapter 2, Section (B)

Choose a Suitable Cloud Service Provider (CSP)

In deciding on your CSP, your agency should be aware of the security and compliance challenges that are unique to cloud computing.

Considerations for Choosing a Cloud Service Provider (CSP)

Checklist	Steps
Ensure CSP is compliant with Singapore standards	• Obtain a copy of the Multi-Tier Cloud Security (MCTS) Certification from the CSP.
Perform risk assessment and ensure CSP has baseline security controls in place	• Request CSP to present its cybersecurity and data protection measures. • Consider internal systems integration needs. Your agency should be aware about the connectivity aspect and whether the impacted software is compatible or consider upgrades. • Ask existing appointed software service providers and the commercial CSP to weigh its offerings against your agency's requirement and risk appetite.
Be aware of application of laws to personal data stored in cloud servers and its jurisdiction	• Ensure adequate security protection for personal data under your agency's possession, and that all ethical, professional, and legal obligations are maintained.

Chapter 2, Section (B)

Checklist	Steps
Be aware of application of laws to personal data stored in cloud servers and its jurisdiction	• Ensure that any overseas transfer of personal data as a result of engaging a CSP will be done in accordance with the requirements under the PDPA i.e. CSP should only transfer data to locations with comparable data protection regimes, or has legally enforceable obligations to ensure a comparable standard of protection for the transferred personal data.

Considerations when using Cloud Services to Process Personal Data

For more information on considerations when using cloud services to process personal data in the cloud, your agency can refer to Section 8: Cloud Services of Advisory Guidelines on the PDPA for Selected Topics.

Good and Enhanced Practices of Cloud Computing

Your agency can refer to Table 10 in Section 14: Cloud Computing of Law Society's Guide to Cybersecurity for Law Practices (under General Resources), for good and enhanced practices of cloud computing.

Cloud computing's added flexibility also entails potential vulnerabilities, and hence extra attention should be given when implementing a security strategy. Communication between your agency and the CSP (in particular, the service agreement), should clearly delineate those security responsibilities.

Chapter 2, Section (C)

Understand Ways to Protect Stored Data

It is crucial for your agency to implement robust end-to-end security measures for cloud environment, considering the prevalence of personal data in the social service sector.

When protecting data residing in end-point devices (e.g. laptops, mobiles, Internet of Things (IoTs)) or on-site server/storage and equipment, your agency can adopt techniques such as implementing physical safeguards, conducting regular testing, and protecting access to storage systems:

Good and Enhanced Practices of End-to-End Security

Checklist	Good and Enhanced Practices
End-point Devices	Refer to Section 5B: Personal Computers, Portable Computing Devices and Removable Storage Media of Data Protection Guide for Charities: Managing and Securing Electronic Personal Data (under Guides)
Regular Testing of ICT System	Refer to Section on ICT Controls (ICT Security and Testing) of Guide to Data Protection Practices for ICT Systems
Computer Networks	Refer to the following: • Chapter 8: Computer Networks of Law Society's Guide to Cybersecurity for Law Practices (under General Resources) • Section on ICT Controls (Computer Networks) of Guide to Data Protection Practices for ICT Systems.

Chapter 2, Section (C)

Checklist	Good and Enhanced Practices
Access Controls	Refer to Section 5A: Implementing Controls and Limiting Access to Personal Data of Data Protection Guide for Charities: Managing and Securing Electronic Personal Data (under Guides)

Once your agency chose the suitable CSP and secured the environment from harmful intrusions, safeguards against human errors should be implemented to protect the confidentiality, usability, and integrity by establishing internal information and communications technology (ICT) and data policies and practices.

Your agency can consider adopting these practices to protect integrity of your stored data:

Security Measures	How does this help protect integrity of stored data?
Encryption	Protects stored data from being accessed by unauthorised parties, through the process of encoding information. Your agency should ensure effective encryption by: • Managing and protecting encryption keys well, including keeping the encryption key secure and separate from the encrypted • Review the method of encryption (e.g. algorithm and key length) periodically to ensure that it is recognised by the industry as relevant and secure Encryption of data at rest can be done at the: • Database (transparent to application); and • Application before storing data in the database. Decryption at the application is required after retrieving from the database

Chapter 2, Section (C)

Security Measures	**How does this help protect integrity of stored data?**
Hashing	Facilitates the storing of data items without necessarily reading them again i.e. passwords and email-addresses Hashing generates a string of a fixed length from a text using algorithms. Unlike encryption, the reliability of hashing algorithms does not depend on access to an encryption key, and therefore eliminates the risks incurred when a key is stolen
Software to detect and log unauthorised use	Helps trigger audit alerts when unauthorised uses occur
Due diligence on CSP	Stipulates CSP, by indicating in the service agreement, to take specific data protection measures required to protect the personal data entrusted to it (e.g. encryption of database, not storing the full string of NRIC numbers)
Anti-malware software	Helps scan computer systems to prevent, detect and remove malware

Systems-in-built Mechanisms to Protect Data Integrity

For more information on other systems-in-built mechanisms to protect data integrity during data storage, your agency can refer to the following guides:

- Chapter 10: Data Management of Law Society's Guide to Cybersecurity for Law Practices (under General Resources); and
- Appendix IX: Security Measures to Protect Data Integrity of Trusted Data Sharing Framework.

Chapter 2, Section (C)

To avoid any unrecoverable loss or corruption of electronic data, your agency should:

- Establish a data backup policy and process. Creating regular backups will enable your agency to recover data in event of accidental data deletion due to human errors or data corruption due to hardware/software failures etc.

Factors for Consideration in Establishing a Data Backup Policy

In establishing a data backup policy, your agency should evaluate:

- Type of data to be backed up
- Size of the data
- Frequency of data backup
- Storage for backed up data

Note: Backups can be stored onsite or on the cloud, however in choosing the latter, your agency should ensure full understanding of the cloud-based backup services provided by your CSP.

- Develop an incident response and reporting plan. Having a plan will allow your agency to effectively manage incidents where your ICT system or data is compromised.

Cyber Incident Response and Reporting

For guidance on how your agency may contain and recover from an incident quickly and efficiently, refer to Annex C: Cyber Incident Response Checklist of the Guide to Managing and Notifying Data Breaches Under the PDPA. For incident reporting, your agency can refer to Section 5.2(b): Incident Reporting of the Cybersecurity Essentials for Social Service Agencies and Charities.

Chapter 2, Section (C)

Continuing Education and Training (CET) Programmes in Cybersecurity (funded by SkillsFuture Singapore (SSG))

If your agency requires more assistance in area of cybersecurity, you can consider enrolling into SSG-funded CET programmes in Cybersecurity. Your agency can leverage on the mentoring and projects/assignments in these courses to develop customised templates for IT security policies and data management guidelines.

Chapter 2, Section (D)

Understand Personal Data Protection Act Obligations in Data Storage

The Personal Data Protection Act (PDPA) governs the collection, use and disclosure of personal data by agencies in a manner that recognises both the right of individuals to protect their personal data and the need of agencies to collect, use or disclose personal data for purposes that a reasonable person would consider appropriate in the circumstances.

> "Personal data" means data, whether true or not, about an individual who can be identified –
>
> (a) From that data; or
>
> (b) From that data and other information to which the organisation has or is likely to have access.

PDPA Obligations to Highlight when Storing Personal Data

Key things to note when storing personal data:

PDPA Obligations	How can your agency comply with the PDPA obligations?
Accuracy Obligation	• Ensure strict access controls are in place to prevent any unauthorised alteration to stored data. Access to authorized personnel should only be granted on a 'need-to-know' basis
Protection Obligation	• Implement security measures that can protect data from intrusions as well as corruption. Examples include encrypting electronic files that contain personal data, using relevant software and setting strong passwords

Chapter 2, Section (D)

PDPA Obligations	How can your agency comply with the PDPA obligations?
Protection Obligation	• Store personal data in only agency-issued devices, as well as agency-issued encrypted portable storage media and/or agency's secure storage application • Set up a data backup policy and process in the event of data leakage • Ensure backup is properly secured and destroyed when no longer needed
Data Breach Notification Obligation	• Assess whether data breach is notifiable within a recommended period of 30 calendar days • Notify the Personal Data Protection Commission (PDPC) and/or affected individuals (after notifying PDPC) no later than 3 calendar days, if data breach is assessed to be notifiable Submit the notification at https://eservice.pdpc.gov.sg/case/db. For urgent notification of major cases, your agency may also contact the PDPC at +65 6377 3131 during working hours.

Chapter 2, Section (D)

Data Protection and Cybersecurity Consultancy Grant

Your agency can tap on the Data Protection and Cybersecurity Consultancy Grant to uplift your data protection and cybersecurity standards. The consultancy will be provided by the pre-appointed consultant, in individual modules that you can select based on your needs and budget. Funding support is provided up to 80%, capped at $40,000 or $60,000 per track, depending on the scope of work.

Data Protection Trustmark (DPTM)

Your agency can apply for the Data Protection Trustmark (DPTM), a voluntary enterprise-wide certification (administered by IMDA), that helps to establish and recognise robust data governance standards by encouraging accountability and strengthening compliance. If equipped with DPTM, your agency will be better positioned to build trust with your users, as it will help to boost confidence in the agency's management of personal data.

CHAPTER 3: USE DATA

CHAPTER 3: USE DATA

Data contributes to knowledge building and when well leveraged, can be used for various needs such as to identify trends and gain actionable insights on service users' needs, enhance service planning, operations and quality of existing services etc.

Overview

Focus on data usage in an efficient and responsible manner

- Verify Purpose for Data Usage
- Understand Ways to Use Data
- Establish Internal Protocols and Procedures for Data Usage
- Understand Personal Data Protection Act (PDPA) Obligations in Data Usage

Checklists

Help your agency meet minimal baselines

- Considerations for Developing Internal Policies for Data Usage
- PDPA Obligations to Highlight when Using Personal Data

Resources

Apprise on other guidelines and support related to data usage

Your agency should adopt the concepts in this guide, along with the following resources:

- Anonymisation of Personal Data for Use
- Data Protection and Cybersecurity Consultancy Grant

Chapter 3, Section (A)

Verify Purpose for Data Usage

Before using data, your agency should verify the purpose for data usage:

1. Establish the purpose of using the data.
2. Check that your agency has the data required to fulfil the established purpose.
3. Ensure that data is kept up-to-date and accurate.
4. Check against your agency's internal data policies to verify that the data can be used for the established purpose.

   You can refer to Chapter 3, Section (C) for more information on internal data policies.

Understand Ways to Use Data

Data is the new oil. Like oil, data is valuable, but if unrefined, it cannot really be used. Below are broad suggestions on how data can help your agency to:

(I) Extract Actionable Insights to Improve Services through Data Analytics

(II) Improve Agency's Operational Efficiency with up-to-date Information

(I) Extract Actionable Insights to Improve Services through Data Analytics

Data can be used to drive the following analysis:

Types of Data Analysis Method	Benefit to Your Agency	Process/ Techniques
Descriptive (What happened)	Informs past happenings by providing context to interpret raw information	Data visualisation i.e. graphs, charts and reports
Exploratory (How to explore data relationships)	Uncovers patterns, spots anomalies, and forms connections between datasets	Data discovery
Diagnostic (Why it happened)	Gives contextual understanding of root causes underlying data, providing direct and actionable answers to specific questions	Data mining, drill down and drill through
Predictive (What will happen)	Predicts future data by applying historical data on current data	Machine learning
Prescriptive (How will it happen)	Suggests courses of action and outlines corresponding potential implications	Predictive modelling

More details on data analysis methods and techniques can be found here.

Chapter 3, Section (B)

In cases where data intended for use constitutes personal data, your agency must put in place risk management controls in order to use and process personal data in compliance with the Personal Data Protection Act (PDPA). One way is to use data in an anonymised form – Anonymised data is not personal data and thus will not be governed by the PDPA.

Anonymisation of Personal Data for Use

Anonymisation refers to the process of converting personal data into data that cannot be used to identify any particular individual:

When anonymising personal data, your agency should:

1. Determine the extent to which the data itself can be anonymised effectively or meaningfully.
2. Consider anonymisation techniques available, taking into account the intended use of data as well as your organisation's capabilities.
3. Apply the appropriate anonymisation techniques to ensure robust anonymisation of the data.

Refer to Advisory Guidelines on the PDPA for Selected Topics for more information on:

- Section 2: Analytics and Research – Considerations when conducting analytic and research activities involving personal data.
- Section 3: Anonymisation – Anonymising personal data, including anonymisation techniques.

Chapter 3, Section (B)

(II) Improve Agency's Operational Efficiency with up-to-date Information

Having up-to-date information can help improve organisational efficiency. Your agency should conduct regular data updates to ensure a single source of truth which can improve efficiency in the following ways, e.g.:

Save time and effort in verifying with users on their information when assessing applications

Ensure consistency in staff assessment of users' eligibility for services with fixed eligibility criteria

Demonstrate accountability to stakeholders by meeting legal compliance-driven requirements through data upkeeping

Support in efficient planning of resource and new services

Chapter 3, Section (C)

Establish Internal Protocols and Procedures for Data Usage

An internal data policy should serve to clarify internal protocols and procedures when using data across the agency.

Having "rules of the road" in place will assist and make efficient the sourcing and use of data within the organisation and across units.

When considering such policy, your agency should consider, but not limited to, the three key following aspects:

Considerations for Developing Internal Policies for Data Usage

Checklist	Steps your agency can take	How does these steps clarify internal policies?
Develop a clear documentation of data	Capture sufficient metadata (descriptive information)	• Helps staff discover, identify and use data
	Establish shared data dictionary to help locate and build data	• Facilitates standardisation by documenting common data structures the precise vocabulary needed for discussing specific data elements • Ensures that definition, relevance, and quality of data elements are the same for all users (i.e. staff of your agency) to facilitate data requests from other units by: ○ Avoiding confusion and ○ Ensuring that data requested aligns with the data provided

Chapter 3, Section (C)

Checklist	Steps your agency can take	How does these steps clarify internal policies?
Ensure a smooth process of data transmission and management across staff	Establish data classification levels and associated access rights to staff groups	• Helps staff in seeking access rights when obtaining data from other units
	Inform and educate all staff of data protection policies (via posters, email and other communication tools etc)	• Helps staff put policies into practice • Reminds staff of the necessary actions to take to safeguard personal data, especially if handling data is part of their day-to-day work activities
Ensure compliant use, access and transfer of data	Build a data dashboard	• Updates your agency of common or regular information needs in a systemic manner • Helps your agency align and generate common discussions and understanding of data across the agency, which in turn can support further objectives

Chapter 3, Section (C)

Data Protection and Cybersecurity Consultancy Grant

Your agency can tap on the Data Protection and Cybersecurity Consultancy Grant to uplift your data protection and cybersecurity standards. The consultancy will be provided by the pre-appointed consultant, in individual modules that you can select based on your needs and budget. Funding support is provided up to 80%, capped at $40,000 or $60,000 per track, depending on the scope of work.

Chapter 3, Section (D)

Understand Personal Data Protection Act Obligations in Data Usage

The Personal Data Protection Act (PDPA) governs the collection, use and disclosure of personal data by agencies in a manner that recognises both the right of individuals to protect their personal data and the need of agencies to collect, use or disclose personal data for purposes that a reasonable person would consider appropriate in the circumstances.

> "Personal data" means data, whether true or not, about an individual who can be identified –
>
> (a) From that data; or
>
> (b) From that data and other information to which the organisation has or is likely to have access.

PDPA Obligations to Highlight when Using Personal Data

Key things to note when using personal data:

PDPA Obligations	How can your agency comply with the PDPA obligations?
Consent Obligation	• Obtain fresh consent for the intended use of data if it differs from the original purpose previously consented.
Purpose Limitation Obligation	• Use personal data that are relevant for the intended purposes, and only for purposes that are reasonable.
Notification Obligation	• Inform individual of the purposes for the use of data, on or before such use.

Chapter 3, Section (D)

PDPA Obligations	How can your agency comply with the PDPA obligations?
Access and Correction Obligation	• Allow individuals to correct data error or omission. • Provide information relating to how data has or may have been used within the past year, in response to specific access request. • Consider what a reasonable person would consider appropriate in the circumstances and use your best judgment when handling access request to his/her own data.
Accuracy Obligation	• Ensure data is accurate before using it to make decisions affecting individuals. • Ensure source is legitimate before allowing any updates.
Protection Obligation	• Limit access to personal data on a need to know basis. • Process personal information out of sight of unauthorised personnel. • Anonymise data as much as possible before analysis, or release only aggregated results. Refer to Chapter 3, Section (B). • Ensure individual cannot be reidentified from anonymised data. • Keep case files containing personal information under lock and key when not in use, with the key only accessible to authorized personnel.

CHAPTER 4: SHARE DATA

CHAPTER 4: SHARE DATA

Data sharing at the social service sector level is at nascent stage; agencies are only beginning to recognise and explore the value of exchanging and leveraging on each other's data to increase operational efficiency and improve service provisions. Data sharing can help to reduce data silos, improve service intelligence and enable data-driven decision making.

Overview

Focus on sharing data across agencies

- Develop a Purpose for Data Sharing
- Establish a Data Sharing Agreement (DSA)
- Assess Data for Sharing
- Understand Ways to Share Data
- Understand Personal Data Protection Act (PDPA) Obligations in Data Sharing

Checklists

Help your agency meet minimal baselines

- Terms and Conditions in Data Sharing Agreement (DSA)
- Considerations in Developing Data Protection Policy
- PDPA Obligations to Highlight when Sharing Personal Data

Resources

Apprise on other guidelines and support related to data sharing

Your agency should adopt the concepts in this guide, along with the following resources:

- Data Intermediary (DI) Management Lifecycle
- Data Management and Sharing with the Ministry of Social and Family Development (MSF)
- Good Practices for Emails, Websites and Web Applications Security
- Factors for Consideration before Personal Data Sharing

Chapter 4, Section (A)

Develop a Purpose for Data Sharing

A clearly articulated common purpose for data sharing will help your agency to:

1. Assess the potential for data sharing with the identified use case
2. Plan how you can draw insights from the data to achieve your purpose
3. Obtain relevant data for your use or sieving data for sharing

Data Sharing Purposes	Potential Data Required
Provide multi-faceted support to individuals/families' multiple needs	• Assistance schemes relevant to main support provided (potentially with another agency) • Training and employment subsidy schemes • Cross segment needs (i.e. senior, childcare programmes)
Enhance coordination between agencies for referral cases	• Personal particulars • Relevant case details to service the referral • Financial assistance records
Contribute to sector-related research activities	• Metadata for shared data sets • Source and citation of datasets

Chapter 4, Section (B)

Establish a Data Sharing Agreement (DSA)

Having established the potential utility or purpose of data sharing, your agency should then identify the relevant parties. Following which, parties involved should establish and sign a Data Sharing Agreement (DSA).

DSA is required when data is shared outside of your agency. It:

- Documents terms and conditions of data sharing agreed by the parties involved to avoid ambiguity in the data sharing process.
- Determines the parameters for the data permitted for sharing and help govern the data sharing partnership.

Terms and Conditions in Data Sharing Agreement (DSA)

In addition to the important terms of DSA as outlined Section 2.2: Establish Data Sharing Agreement of the Trusted Data Sharing Framework, your agency can consider including the following elements to cover in the DSA:

- Roles and responsibilities of the parties involved
- Purpose for data sharing
- Types of data to be shared (e.g. personal data, programme data)
- Consent provision for sharing of personal data for intended purpose
- Medium for data sharing (e.g. APIs, file transfer via email)
- Processes to facilitate access and correction requests to personal data shared
- Frequency of data sharing (e.g. ad-hoc, one-off exercise, routine process)
- Protocols for data handling/ constraints on data usage where applicable

Note: Your agency can choose to include confidentiality clauses in the DSA or put in a place a stand-alone confidentiality agreement.

Chapter 4, Section (B)

Data Intermediary (DI) Management Lifecycle

A data intermediary refers to an external organisation that is processing data on behalf of your agency. Your agency should ensure that you have all necessary understanding when managing data intermediaries. Your agency can refer to the Guide to Managing Data Intermediaries for more information.

Chapter 4, Section (C)

Assess Data for Sharing

Your agency should assess the data that can be shared with other agencies and prepare them, based on the following documents:

- **Data Sharing Agreement (DSA). Refer to Chapter 4, Section (B).**
- **Personal Data Protection Act (PDPA) (for sharing of personal data). Refer to Chapter 4, Section (E).**
- **Also remember to reference back to your agency's data protection policy.**

  To prepare (compile, refine and anonymise (where applicable)) data for sharing in accordance with the data protection policy, and ensure that the data can be used for the intended purpose.

Considerations in Developing Data Protection Policy

For considerations in developing data protection policy, your agency can refer to Part II: What Should Be in a Policy? of Guide to Developing a Data Protection Management Programme.

Data Management and Sharing with the Ministry of Social and Family Development (MSF)

Your agency may find out more about data sharing with MSF to facilitate the extension of social services and Government subsidies/assistance to service users for:

- More accurate assessment and faster access to assistance.
- Tailored advice on assistance.
- Smoother application for healthcare financing schemes.

Chapter 4, Section (D)

Understand Ways to Share Data

Data can be shared across agencies via:

01 INFORMATION/FILE TRANSFER

via email which is a widely used communication tool, even for confidential and sensitive information.

Due to its prevalent use, it faces common cybersecurity attacks such as phishing and malware attacks. It is thus critical to implement security measures to protect personal data that is often transmitted via (and stored within) emails. Other than emails, files can also be transferred via the Secure File Transfer Protocol (SFTP) which uses secure shell encryption to provide a high level of security for sending and receiving file transfers. Third-party software (i.e. Dropbox, Google Drive, WeTransfer etc.) are also prevalent. However, your agency's ICT policy and systems administrators should provide clear policies and guidelines pertaining to their use.

02 WEBSITES AND WEB APPLICATIONS

can be used to disseminate information and provide services.

It is important to keep in mind that websites and web applications ultimately connect to a database which may contain personal and confidential data, thus extra precaution must be taken to prevent malicious attacks on websites and web applications.

Good Practices for Emails, Websites and Web Applications Security

For more information, including good practices to enhance security of emails, websites and web applications, your agency can refer to Sections 5C: Emails and 5D: Websites and web applications of Data Protection Guide for Charities: Managing and Securing Electronic Personal Data (under Guides).

Chapter 4, Section (D)

03 APPLICATION PROGRAMMING INTERFACES (APIS)

facilitates authorised data exchange via software and through a documented interface.

Some legacy software does not come with in-built API capabilities with other software, as they were built on frameworks that disallow integration with more modern systems. If your agency is considering new systems or software purchases, considering their API capabilities will better ensure interoperability across various systems.

Build Own API

- Acts as a common core to integrate applications
- Can be developed specific to systems and needs
- Methods include utilising open source code

For further reading, refer to the Beginner's Guide to Building API Services here.

Open Source API

- Allows customisation and reduces development time
- Examples include open source digital tools that can be readily accessed, adapted, and modified

More information on the open source technologies and tools available can be found here.

Government API

- Provides safe and convenient access to public datasets
- Enables the linking of agencies' products with Government data and services

More details can be found here.

Chapter 4, Section (E)

Understand Personal Data Protection Act Obligations in Data Sharing

The Personal Data Protection Act (PDPA) governs the collection, use and disclosure of personal data by agencies in a manner that recognises both the right of individuals to protect their personal data and the need of agencies to collect, use or disclose personal data for purposes that a reasonable person would consider appropriate in the circumstances.

> "Personal data" means data, whether true or not, about an individual who can be identified –
>
> (a) From that data; or
>
> (b) From that data and other information to which the organisation has or is likely to have access.

PDPA Obligations to Highlight when Sharing Personal Data

Key things to note when sharing personal data:

PDPA Obligations	How can your agency comply with the PDPA obligations?
Consent Obligation	• Purpose for data sharing is reasonable. • Individual has provided consent to disclosure of his/her personal data by your agency to another agency for the particular purpose.
Purpose Limitation Obligation	• Share or disclose data that are relevant for the intended purposes, and only for purposes that are reasonable.

Chapter 4, Section (E)

PDPA Obligations	How can your agency comply with the PDPA obligations?
Notification Obligation	• Inform individual of purpose for which personal data will be shared, unless exceptions under the PDPA applies. • Ensure that notifications are clear, easily comprehensible, provide appropriate information and are easily accessible. • Inform individual of new purpose if purpose of data sharing falls under a different purpose from which it was collected.
Protection Obligation	• Share required personal data only (in anonymised manner[7], where applicable). Refer to Section 3: Anonymisation of Advisory Guidelines on the PDPA for Selected Topics for more information. • Use a password-protected file with password provided in a separate email, when sharing personal data electronically. • Ensure that clients' personal data is not shared via network file share and personal online services (e.g. iCloud, Dropbox, Google, OneDrive). • Receiving party (internal department within agency or external party) complies with PDPA. • Receiving party (if external party) to be bounded by DSA, to ensure they are accountable to the party sharing the data for the use of that data. Specifically, the DSA should stipulate the obligations in terms of what receiving party can/cannot use the data for, that they should protect the data from unauthorised access, and that they need to destroy the data once purpose is fulfilled etc

[7] Agencies should consider anonymising personal data if purpose can be achieved with the anonymised data.

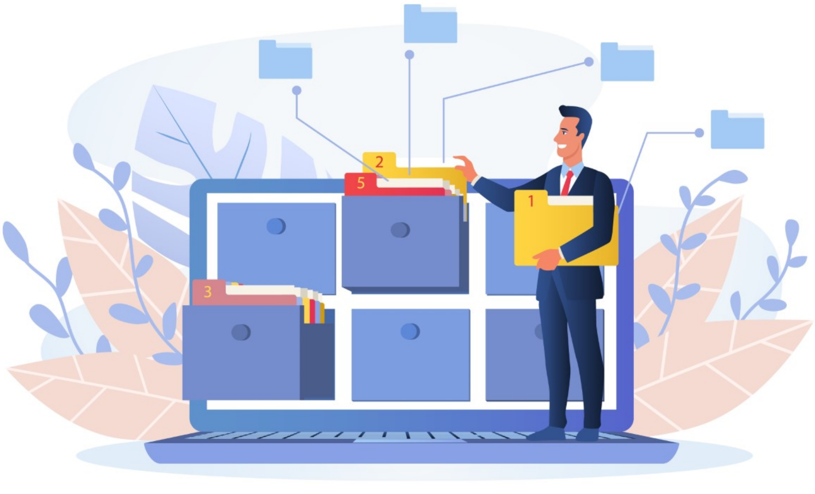
Chapter 4, Section (E)

PDPA Obligations	How can your agency comply with the PDPA obligations?
	• Personal data is shared for intended purpose only. • Personal data is archived/destroyed when no longer needed.
Transfer Limitation Obligation	• Receiving party located outside of Singapore has to be bound by data protection law of that country which is at least equivalent to Singapore PDPA

Factors for Consideration before Personal Data Sharing

For more personal data sharing considerations, your agency can also refer to Part 2: Factors to Consider before Sharing of Guide to Data Sharing.

CHAPTER 5: ARCHIVE/ DESTROY DATA



CHAPTER 5: ARCHIVE/DESTROY DATA

Data, no longer required for active use, should be archived for long-term retention. Upon the end of the required retention period or otherwise confirmed to be no longer required, data should be destroyed. Archiving and destroying data can potentially reduce costs of primary storage and backup through data volume reduction.

Overview

Focus on archiving and destroying data

- Understand the Benefits of Archiving Data
- Assess Data for Archival vis-à-vis Destruction
- Archive and Destroy Data in a Secured Manner
- Understand Personal Data Protection Act (PDPA) Obligations in Data Archival and Destruction

Checklists

Help your agency meet minimal baselines

- Considerations in Archiving and Destroying Data
- Documents Retention Requirements
- PDPA Obligations to Highlight when Archiving and Destroying Personal Data

Resources

Apprise on other guidelines and support related to archival and destruction

Your agency should adopt the concepts in this guide, along with the following resources:

- Data Archival on Clouds
- Retention of Personal Data

Chapter 5, Section (A)

Understand the Benefits of Archiving Data

Agencies accumulate a wealth of data over time, including personal data relating to your users, donors, staff etc.

It is important to regularly assess the need for these data to be preserved. Regardless of the type of storage medium (e.g. removable storage media or servers), your agency can free up primary storage space for other immediate needs, by archiving the data.

Compared to data backups which create replicas of the data in use at the primary location to prevent data loss and corruption, data archival is a process for storing data for long-term retention. Their underlying processes are similar, except data archival does not need to be synchronised with the latest changes in the primary storage location. Instead, it is stored for historical or compliance and legal purposes.

Refer to Chapter 2: Store Data for more information on data backups.

Chapter 5, Section (A)

Your agency can benefit from data archival in the following ways:

Benefits from Data Archival	
Reduce potential costs associated with maintenance and operations	A reduction in volume of primary data required for backup, thereby optimising backup times and costs of primary storage.
Enhance application performance with smaller volume of data on primary storage	A lower data volume on primary storage can minimise overheads on the operating system.
Increase security of data files	A reduction in circulated data files can reduce the chance of data files being compromised by malware infections and cyberattacks.
Prevent data loss	A reduction in ability to modify data stored in the archived data management system can prevent data loss.

Data Archival on Clouds

When archiving data on cloud servers, your agency should understand the pros and cons of offsite archiving solutions.

Chapter 5, Section (B)

Assess Data for Archival vis-à-vis Destruction

Your agency should take note of the following when deciding whether to archive or destroy data:

01 DATA PROFILE

whether data is redundant, trivial, or obsolete

02 YOUR AGENCY'S INTERNAL DATA POLICY ON DATA ARCHIVAL AND DESTRUCTION

03 DOCUMENT RETENTION REQUIREMENTS

stipulated by legislative acts

Chapter 5, Section (B)

01 DATA PROFILE

Unlike archived data, your agency will not be able to retrieve destroyed data. As such, your agency should take extra caution when permanently destroying data.

Three broad considerations in archiving and destroying data are as follows:

Considerations in Archiving and Destroying Data

	Considerations in Archiving and Destroying Data
Redundant	• Data has met its purpose of collection, use and disclosure. • Data is duplicated within the same system or across multiple systems. In such scenarios, your agency should only keep one source of reference.
Trivial	• Data does not serve as evidence of business activity or historical value. • Data does not provide corporate relevant knowledge. • Data does not give rise to business insights.
Obsolete	• Data has been superseded by other information. • Data is inaccurate or invalid. Refer to Checklist: Key Components of Data Quality under Chapter 1, Section (D).

Chapter 5, Section (B)

02 YOUR AGENCY'S INTERNAL DATA POLICY ON DATA ARCHIVAL AND DESTRUCTION

Establishing an internal data destruction policy can ensure all employees are well-versed in best practices when permanently removing data from Information and Communications Technology (ICT) systems. Having clear procedures and protocols will allow your agency to effectively handle different types of data in your possession, while instilling a culture of compliance in the workplace.

Your agency's internal data policy should take into consideration the document retention requirements, which are further elaborated in Point (3) below.

03 DOCUMENT RETENTION REQUIREMENTS

Depending on the nature of the data in question, your agency must consider statutory limitation periods that are applicable. Documents retention requirements will inform of the minimum prescribed period for which the data should be kept for. Your agency should reference those legal requirements applicable (overall or specific to sets of data), including the following more common, but may not be limited to, for agencies:

Document Retention Requirements

Applicable Act or Guidelines	Document Retention Requirements
Co-operative Societies Act	• Maintain proper accounts and records of the transactions and affairs of the society for a period of at least five years. Refer to Part III 32B: Keeping of Records and Documents, etc of Co-operative Societies Act.

Chapter 5, Section (B)

Applicable Act or Guidelines	Document Retention Requirements
Charities Act	• Retain accounting records for five years, as stipulated under the Charities Act. • Adhere to additional requirements applicable to charities e.g. last trustees of the charity are obliged to preserve these documents for five years even where the charity ceased to exist within the five years. Refer to Part IV 12: Duty to Keep Accounting Records of the Charities Act.
Companies Act	• Retain records for a period of not less than 5 years from the end of the financial year in which the transactions or operations to which those records relate are completed. Refer to Part VI 199: Accounting Records and Systems of Control of Companies Act.
MOH regulations, guidelines and circulars	• Adhere to longer retention requirements related to medical records[8]. Refer to Guidelines on the Retention of Medical Records.

[8] Medical records refer to all clinical encounters and original inpatient and outpatient records generated at the time of admission or outpatient attendance.

Chapter 5, Section (C)

Archive and Destroy Data in a Secured Manner

Once your agency has determined that the electronic data is no longer needed, it is crucial to ensure effective and secure destruction of the data, as failure to do so can lead to breaches of data protection and privacy policies, compliance problems and added costs.

When attempting to remove data, it is not as simple as deleting data files residing in the hard drive or in the computer's memory. Your agency must ensure that the deleted files will not be recoverable. Data sanitisation techniques must be robust enough such that data files, once deleted, cannot be retrieved or reconstructed.

Your agency can consider adopting these good practices when archiving or destroying electronic data:

	Good Practices
Archival	• Back up data archives on additional servers by creating multiple copies, if possible. • Check the integrity of archived data regularly to ensure any data corruption do not go unnoticed. • Ensure all archived data adheres to established data retention policies. • Have knowledge about your data to effectively determine data that needs to be easily accessible, and those to be archived. • Enforce high standards by choosing a suitable cloud service provider (CSP), when archiving data on cloud servers. For considerations on choosing a suitable CSP, refer to Chapter 2, Section (B).

Chapter 5, Section (C)

	Good Practices
Destruction	• Use specific software that can overwrite selected files or the entire storage device. • Use specialised hardware appliances (e.g. a degausser machine).

Retention of Personal Data

For more information on good practices in retaining personal data, refer Section on ICT Controls (Retention of Personal Data) of Guide to Data Protection Practices for ICT Systems.

Chapter 5, Section (D)

Understand Personal Data Protection Act Obligations in Data Archival and Destruction

The Personal Data Protection Act (PDPA) governs the collection, use and disclosure of personal data by agencies in a manner that recognises both the right of individuals to protect their personal data and the need of agencies to collect, use or disclose personal data for purposes that a reasonable person would consider appropriate in the circumstances.

> "Personal data" means data, whether true or not, about an individual who can be identified –
>
> (a) From that data; or
>
> (b) From that data and other information to which the organisation has or is likely to have access.

PDPA Obligations to Highlight when Archiving and Destroying Personal Data

Key things to note when archiving and destroying personal data:

PDPA Obligations	How can your agency comply with the PDPA obligations?
Protection Obligation	• Review personal data regularly and dispose of anything that is no longer needed. • Ensure personal data is permanently destroyed.
Retention Limitation Obligation	• Cease the retention of documents containing personal data as soon as it is reasonable to do so.

Chapter 5, Section (D)

PDPA Obligations	How can your agency comply with the PDPA obligations?
Retention Limitation Obligation	• Agencies who choose to retain personal data should anonymise the data for future use. Refer to Section 3: Anonymisation of Advisory Guidelines on the PDPA for Selected Topics for more information. • Do not keep data longer than required as it will increase the risk of unauthorised disclosure. • Consider setting clear data retention periods for the various types of personal data under your agency's possession. Your agency should take note of the document retention requirements (Refer to Chapter 5, Section (B)) when setting data retention periods.

CONCLUSION

This Data Management Guide serves to provide agencies with recommended practices, resources and guidelines on data management from end-to-end data lifecycle perspective. The guide is not meant to be prescriptive, but to support agencies to review, reflect and identify gaps in their current data management practices, and take steps to adopt good practices early.

Thank you!

We thank you for your continued support in our efforts to build sector data capabilities.

Contact

National Council of Social Service
170 Ghim Moh Road,
#01-02, Singapore 279621
Tel: 6210 2500 Fax: 6468 1012
ncss_webmaster@ncss.gov.sg

REFERENCES

Alan Manicom. (2018). An Overview of Data Archiving Best Practices. Redstor (article). Accessed 31 Aug 2021. Retrieved from https://www.redstor.com/en-us/blog/data-archiving-best-practice-overview/

Alan Manicom. (2018). Archive or Delete - What Should You Do With Your Data?. Redstor (article). Accessed 1 Oct 2021. Retrieved from https://www.redstor.com/blog/archive-or-delete-what-should-you-do-with-your-data/

Bernardita Calzon. (2021). Data Analysis Methods and Techniques. Datapine (article). Accessed 1 Oct 2021. Retrieved from https://www.datapine.com/blog/data-analysis-methods-and-techniques/

Cloudian. (2021). Data Backup & Archive. Cloudian (article). Accessed 31 Aug 2021. Retrieved from https://cloudian.com/guides/data-backup/data-archive/

Commissioner of Charities. (2020). Data Protection Guide for Charities: Managing & Securing Electronic Personal Data. Accessed 1 Oct 2021. Retrieved from https://www.charities.gov.sg/PublishingImages/Resource-and-Training/Guides-Templates-Awards/Guides/Documents/Data%20Protection%20Guide%20for%20Charities%20Managing%20&%20Securing%20Electronic%20Personal%20Data.pdf (under Guides)

Infocomm Media Development Authority (IMDA). (2014). Multi-Tier Cloud Security (MTCS) Certification Scheme. Accessed 1 Oct 2021. Retrieved from https://www.imda.gov.sg/regulations-and-licensing-listing/ict-standards-and-quality-of-service/IT-Standards-and-Frameworks/Compliance-and-Certification

Infocomm Media Development Authority (IMDA). (2019). Data Collaboratives Programme. Accessed 30 Oct 2021. Retrieved from https://www.imda.gov.sg/programme-listing/data-collaborative-programme

Infocomm Media Development Authority (IMDA). (2019). Data Protection Trustmark Certification. Accessed 1 Oct 2021. Retrieved from https://www.imda.gov.sg/programme-listing/data-protection-trustmark-certification

Infocomm Media Development Authority (IMDA). (2019). Trusted Data Sharing Framework. Accessed 1 Oct 2021. Retrieved from https:/www.imda.gov.sg/-/media/Imda/Files/Infocomm-Media-Landscape/SG-Digital/Tech-Pillars/Artificial-Intelligence/Trusted-Data-Sharing-Framework.pdf

Lauren Witley. (2016). 5 Crucial Reasons to Keep Your Data Up to Date. DataClarity (article). Accessed 20 Aug 2021. Retrieved from https://www.dataclarity.uk.com/2016/03/03/5-crucial-reasons-to-keep-your-data-up-to-date/

Maxwell Cooter. (2021). Cloud Archiving: A Perfect Use Case, but Beware Costs and Egress Issues. ComputerWeekly (article). Accessed 31 Aug 2021. Retrieved from https://www.computerweekly.com/feature/Cloud-archiving-A-perfect-use-case-but-beware-costs-and-egress

Ministry of Health. (2015). 2015 Guidelines for the Retention Periods of Medical Records. Accessed 1 Oct 2021. Retrieved from https://www.moh.gov.sg/resources-statistics/guidelines/2015-guidelines-on-the-retention-of-medication-records

Ministry of Social and Family Development (MSF). (2018). Data Security Instructions for Agencies Running MSF-Funded Programmes. Accessed 1 Oct 2021.

REFERENCES

Ministry of Social and Family Development (MSF). (2021). Data Management and Sharing. Accessed 1 Oct 2021. Retrieved from https://www.msf.gov.sg/policies/Social-Service-in-Singapore/Pages/Data-Management-and-Sharing.aspx

National Council of Social Service (NCSS). (2021). Data Protection and Cybersecurity Consultancy Grant. Accessed 1 Oct 2021. Retrieved from https://www.ncss.gov.sg/our-initiatives/tech-and-go/consultancy

National Council of Social Service (NCSS). (2021). Cybersecurity Essentials for Social Service Agencies and Charities. Accessed 1 Oct 2021. Retrieved from https://www.ncss.gov.sg/press-room/publications/industry-digital-plan-for-social-services

Personal Data Protection Commission (PDPC). (n.d.). Data Protection Notice Generator. Accessed 1 Oct 2021. Retrieved from https://apps.pdpc.gov.sg/dp-notice-generator/introduction

Personal Data Protection Commission (PDPC). (n.d.). PDPA Assessment Tool for Organisations (PATO). Accessed 29 Oct 2021. Retrieved from https://apps.pdpc.gov.sg/resources/pato

Personal Data Protection Commission (PDPC). (n.d.). Sample Personal Data Inventory Map Template. Accessed 1 Oct 2021. Retrieved from https://www.pdpc.gov.sg/Help-and-Resources/2019/07/Guide-to-Developing-a-Data-Protection-Management-Programme/Resources

Personal Data Protection Commission (PDPC). (2018). Advisory Guidelines for the Social Service Sector. Accessed 1 Oct 2021. Retrieved from https://www.pdpc.gov.sg/guidelines-and-consultation/2018/09/advisory-guidelines-for-the-social-service-sector

Personal Data Protection Commission (PDPC). (2018). Guide to Data Sharing. Accessed 1 Oct 2021. Retrieved from https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Other-Guides/Guide-to-Data-Sharing-revised-26-Feb-2018.pdf

Personal Data Protection Commission (PDPC). (2019). Advisory Guidelines on Personal Data Protection Act for Selected Topics. Accessed 1 Oct 2021. Retrieved from https://www.pdpc.gov.sg/guidelines-and-consultation/2020/02/advisory-guidelines-on-the-personal-data-protection-act-for-selected-topics

Personal Data Protection Commission (PDPC). (2020). Guide to Managing Data Intermediaries. Accessed 1 Oct 2021. Retrieved from https://www.pdpc.gov.sg/help-and-resources/2020/09/guide-to-managing-data-intermediaries

Personal Data Protection Commission (PDPC). (2021). Advisory Guidelines on Key Concepts in the Personal Data Protection Act. Accessed 1 Oct 2021. Retrieved from https://www.pdpc.gov.sg/guidelines-and-consultation/2020/03/advisory-guidelines-on-key-concepts-in-the-personal-data-protection-act

Personal Data Protection Commission (PDPC). (2021). Data Protection Officers. Accessed 1 Oct 2021. Retrieved from https://www.pdpc.gov.sg/overview-of-pdpa/data-protection/business-owner/data-protection-officers

REFERENCES

Personal Data Protection Commission (PDPC). (2021). Data Protection Practices for ICT Systems. Accessed 1 Oct 2021. Retrieved from https://www.pdpc.gov.sg/Help-and-Resources/2021/08/Data-Protection-Practices-for-ICT-Systems

Personal Data Protection Commission (PDPC). (2021). E-Learning Programme. Accessed 1 Oct 2021. Retrieved from https://www.pdpc.gov.sg/Help-and-Resources/2018/01/E-Learning-Programme

Personal Data Protection Commission (PDPC). (2021). Guide to Developing a Data Protection Management Programme. Accessed 1 Oct 2021. Retrieved from https://www.pdpc.gov.sg/help-and-resources/2019/07/guide-to-developing-a-data-protection-management-programme

Personal Data Protection Commission (PDPC). (2021). Guide to Managing and Notifying Data Breaches under the PDPA. Accessed 1 Oct 2021. Retrieved from https://www.pdpc.gov.sg/help-and-resources/2021/01/data-breach-management-guide

Ratros Y. (2019). Building API Services: A Beginner's Guide. Google Cloud – Community (article). Accessed 27 Aug 2021. Retrieved from https://medium.com/google-cloud/building-api-services-a-beginners-guide-7274ae4c547f

Rich Castagna. (2021). What is Cloud Backup and How does it Work?. TechTarget (article). Accessed 19 Aug 2021. Retrieved from https://searchdatabackup.techtarget.com/definition/cloud-backup

RSI Security. (2019). Top 5 Disadvantages of Cloud Storage. RSI Security (article). Accessed 24 Aug 2021. Retrieved from https://blog.rsisecurity.com/top-5-disadvantages-of-cloud-storage/

Salesforce. (2021). 12 Benefits of Cloud Computing. Salesforce (article). Accessed 2 Aug 2021. Retrieved from https://www.salesforce.com/ap/products/platform/best-practices/benefits-of-cloud-computing/

Silvia Valcheva. (n.d.). Data Collection Methods & Tools: Advantages And Disadvantages. Intellspot (article). Accessed 26 Jul 2021. Retrieved from http://www.intellspot.com/data-collection-methods-advantages/

Singapore Government Developer Portal. (2021). Data and APIs. Accessed 27 Aug 2021. Retrieved from https://www.developer.tech.gov.sg/technologies/data-and-apis/overview

Singapore Government Developer Portal. (2021). Open-source Technologies. Accessed 27 Aug 2021. Retrieved from https://www.developer.tech.gov.sg/technologies/open-source/

Singapore Statutes Online. (2006). Companies Act. Accessed 1 Oct 2021. Retrieved from https://sso.agc.gov.sg/Act/CoA1967

Singapore Statutes Online. (2007). Charities Act. Accessed 10 Aug 2021. Retrieved from https://sso.agc.gov.sg/Act/CA1994

Singapore Statutes Online. (2009). Co-operative Societies Act. Accessed 1 Oct 2021. Retrieved from https://sso.agc.gov.sg/Act/CSA1979

REFERENCES

SkillsFuture Singapore (SSG). (2020) National Infocomm Competency Framework. Accessed 1 Oct 2021. Retrieved from https://www.ssg.gov.sg/wsq/Industry-and-Occupational-Skills/National-Infocomm-Competency-WSQ.html

Tableau. (2021). Guide To Data Cleaning: Definition, Benefits, Components, And How To Clean Your Data. Tableau (article). Accessed 26 Jul 2021. Retrieved from https://www.tableau.com/learn/articles/what-is-data-cleaning

The Law Society of Singapore. (2020). Document Retention Requirements. Accessed 10 Aug 2021. Retrieved from https://www.lawsocprobono.org/Pages/CIP-Document-Retention-Requirements.aspx

The Law Society of Singapore. (2020). Law Society's Guide to Cybersecurity for Law Practices. Accessed 1 Oct 2021. Retrieved from https://www.lawsociety.org.sg/lss-risk-management-framework-resources/ (General Resources)

Vijay Kanade. (2021). Cloud vs. on-Premise Comparison: Key Differences and Similarities. Toolbox (article). Accessed 2 Aug 2021. Retrieved from https://www.toolbox.com/tech/cloud/articles/cloud-vs-on-premise-comparison-key-differences-and-similarities/