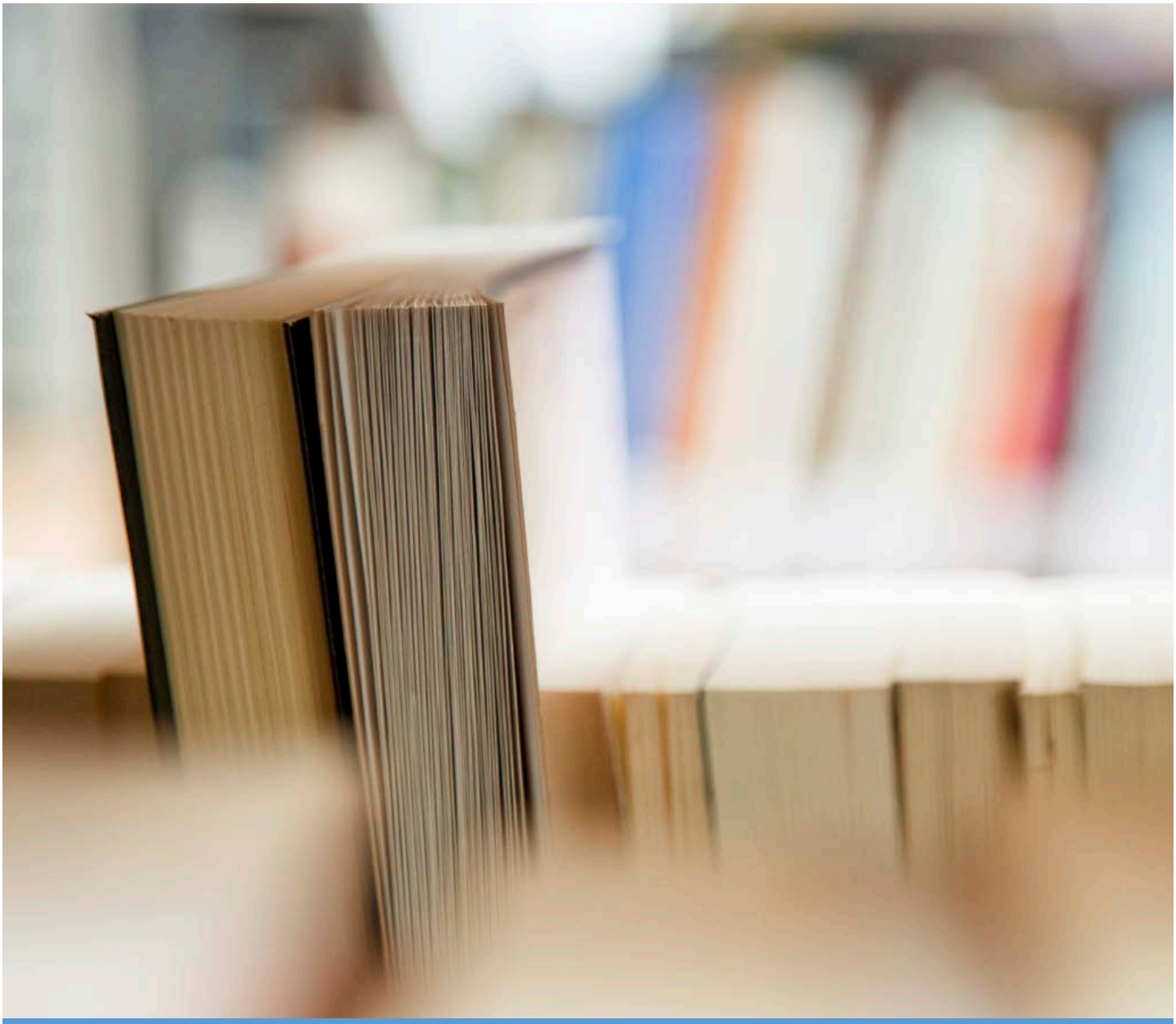

RECORDS MANUAL AND PROCEDURES

National University of Samoa

ESRO Cristina Tuiletufuga

Ver.0.4 (Last modified 16 January 2017)

TABLE OF CONTENTS

GUIDELINE 1: CREATING AND KEEPING RECORDS

THIS IS A RECORDS MANUAL AND PROCEDURES GUIDELINE

FOR **ALL** NUS STAFF.

Introduction

The National University of Samoa Records Manual and Procedures is adapted from the Government of Samoa Code of Best Practice – Records Management. National University of Samoa is considered "*Public Entity*" under "*Public Bodies Act 2001 (Performance and Accountability)*" under Schedule1 Section B. Though this Act, National University of Samoa's records are considered public records and must follow "Public Records Act 2011". This National University of Samoa's Records Manual and Procedures helps all National University of Samoa's staff to keep accurate and complete records of their activities.

This includes:

- abiding to the laws protecting public records
- creating records of all activities done in the service of National University of Samoa
- making sure records are captured in the system
- keeping records in a structured way so they can be found
- keeping records safe
- supporting the work of the records management staff
- fulfilling any specific recordkeeping responsibilities of their positions.

What are records?

Records are "information created, received, and maintained as evidence and information by an organisation or person, in pursuance of legal obligations or in the transaction of business".

The Australian Standard for Records Management (AS ISO 15489:2002)

Abide to the laws protecting public records

Never:

without lawful authorisation abandon or dispose of a public record; or

(a) without lawful authorisation transfer or offer to transfer, or be a party to arrangements for the transfer of, the possession or ownership of a public record; or
(b) without lawful authorisation take or send a public record out of Samoa; or
(c) without lawful authorisation damage or alter a public record; or

(d) knowingly neglect a public record in a way that causes or is likely to cause damage to the public record; or
(e) contravene any conditions of access restriction or special access arrangements to records.

The above activities, because of their seriousness, will be considered criminal offences under the **Public Records Act 2011** (Part10 Offences and Penalties)

All other legal provisions for recordkeeping in Samoan legislation (e.g. in Public Finance Management Act 2001) also must be adhered to.

Create records of all activities:

a. Make sure that detailed minutes of all official meetings are written and approved.
b. Make a note of any discussions, decisions or information received on work issues, e.g. by making a written note on the outcome of phone calls, or by confirming the outcome of discussions in a written letter.
c. Submit reports on the progress of projects.
d. Create full records: Records should always have a document name, page numbers, a date, a File Classification category assigned.
e. If there are different versions of a document, they need to be clearly marked (e.g. Ver1.0, draft, final).

Make sure records are captured in the system:

a. Do not create your own files for National University of Samoa's records, which are not captured in the NUS Classification Scheme.
b. Register all outgoing correspondence in the proper way, so a copy can be filed.
c. Records looked after by all National University of Samoa's Department/sections records (in the Finance Department Library, Oloamanu Centre, Students Administration and Human Resources department, etc.) are also public records. All these units need to cooperate for transparent and accountable recordkeeping. Closed files normally should be given in the custody of the central records unit.
d. Print out e-mail documenting relevant work related issues for filing (Refer to *Guideline 8 – Managing Email* for more information).
e. Do not use post-it notes for notes which will become records (e.g. an approval). They will fall off and get lost.

Make sure records can be found:

a. Keep your electronic files in electronic folders matching NUS Classification Scheme (Refer to *Guideline 7 – Managing Electronic Records* for details).
b. Clearly title electronic files, including clear indication of version (e.g. draft, final)
c. Clearly label discs, photographs, video tapes and other media.
d. Do not clutter your desk:
    - Deal with files promptly and file them when they are no longer required.
    - If applicable, transfer them to the Central Records Unit (after 12 months), so files can be archived when they are not actively used.
    - Remove non-record material such as newsletters, magazines, books and private papers from your desk and keep them on shelves in folders or in your division library.

Keep records safe:

a. Keep your work area clean and free of food and drinks.
b. Handle records gently with clean, dry hands.
c. Do not smoke in areas where records are kept.
d. Do not store any records on the floor.
e. Keep computer equipment including UPS off the floor.
f. Make back-up copies of your computer work.
g. When a staff member resigns or is leaving on long leave PDL, the Manager/Director/ Dean must assure that all the person's records that he did on behalf of National University of Samoa (electronic files and paper files) are saved or transferred to the Central Records Unit. This will be action when the Manager/Director/Dean is informed on the date of resignation.
h. Make sure only authorised people can view access restricted records (refer to, *Guideline 2 –Access* for more details):
    - do not open any envelope or folder marked confidential unless you are sure you are authorised to do so
    - keep any access restricted files locked away when not used
    - mark confidential correspondence clearly
    - advise the Central Records Unit if an access restriction is required.

Support the work of the Central Records Unit:

a. Do not submit material for filing which is subject to Normal Administrative Practice, e.g. editing drafts, or duplicate copies. (*Guideline 13 – Normal Administrative Practice* for more information.)
b. Include the relevant file reference on all records you create.
c. Advise Executive Secretariat Records Officer when a new file should be created, and suggest a clear descriptive title.
d. Cooperate fully with all necessary record checks, including any audits or searches
e. Follow the NUS Records Policy, NUS File Classification Scheme, NUS Retention Schedule and NUS Manual and Procedures approved by Vice Chancellor's Committee and NUS Council and participate in any related trainings/workshops.

Fulfil your specific records management responsibilities:

Vice Chancellor

The Vice Chancellor of National University of Samoa has the overall supervisory function for all activities of the NUS, including recordkeeping. He authorises records transfer and disposal and the access restrictions for archival records. He receives regular reports on records management issues and take appropriate action.

Senior Management

The Vice Chancellor and Senior Management are responsible for the allocation of sufficient resources as required to fulfil recordkeeping obligations. This includes material, equipment, human resources and appropriate storage and working spaces. Every records unit (sections of NUS where they store their own records) needs to have designated staff with relevant Job Descriptions. Records storage rooms need to meet the conditions as set out in *Guideline 10 - Records Storage Rooms*.

All senior managers are responsible for ensuring that their divisions follow the NUS Records Management System (includes: NUS Records Policy, NUS File Classification Scheme, NUS Retention Schedule and NUS Records Manual and Procedures).

Corporate Service Staff

Accounts and Human Resource units may have custodianship over NUS records in their area of work. They need to follow the applicable guidelines of this NUS Records Manual and Procedures concerning the creation, management, storage and disposal of their records, both paper and electronic records, in cooperation with the Executive Secretariat Records Officer.

Records Staff

EXECUTIVE SECRETARIAT RECORDS OFFICER* in NUS is responsible for all aspects of records management, including the design, implementation and maintenance of records systems and their operations, and for training users on records management and records systems operations. Records staff may include not only the EXECUTIVE SECRETARIAT RECORDS OFFICER from Central Records Unit, but also any staff responsible for managing other records units (e.g. land files, court files, personnel files, student files, financial documents etc.) and staff who have aspects of records management as part of their duties, e.g. secretaries, admin assistants, executive assistants…etc.

IT System Managers/Administrators

In this function, they are responsible for making sure that recordkeeping requirements are met in all information systems that they are managing. They need to work closely with the Central Records Unit of the NUS.

Media Unit Managers

The Media Unit store NUS recordings and productions. These sound and visual recordings and photographs are public records and therefore need to be labelled and registered, in cooperation with the EXECUTIVE SECRETARIAT RECORDS OFFICER. The Media Unit is also responsible

for the preservation of NUS recordings, which may involve transfer to another media (e.g. from magnetic tape to more durable digital forms).

GUIDELINE 2: ACCESS

This document provides guidelines on the two main types of access restrictions:

A. Access Restrictions for confidential documents in use at the NUS; and

B. Access Restrictions for closed files which are Archived.

NUS records are public records. The public therefore has a right to access information contained in them. However, not all NUS records can be made accessible to the public. Some even need to be restricted within the NUS sections/departments. In these cases, formal access restrictions have to be placed on records, files or classes of records.

Access restrictions should protect:

- The privacy rights of individuals – *e.g. private information contained in Personal Files*
- Confidential business information – *e.g. tender submissions, contracts made in confidence*
- Security matters – *e.g. building and compound security plans, access codes, special intervention plans*
- Information given or matters discussed under confidentiality – *e.g. Cabinet meeting papers, international relations, performance appraisal documents*
- Information which is part of a current investigation, – *e.g. irregularity investigations, audit.*

Access restriction decisions are important; therefore, they should not be made without due consideration given to all the above issues. In general, information which can be open to a group of people or the public needs to be open to them.

If an access restriction is necessary, the restriction has to be made in an informed and accountable way, and it has to be ensured that this restriction is upheld by all people involved.

A. Making and Managing Access Restrictions on Current Records

The need for access of staff to confidential files depends on the functions of a NUS section/ department; Here fore, each section/ department is responsible for making access restrictions for its own records, collaborating with the EXECUTIVE SECRETARIAT RECORDS OFFICER.

The usual access restrictions given are:

- Vice Chancellor only
- Senior Management only
- Human Resource Unit only
- DVC Corporate Services only
- DVC Academic and Research only
- Executive Secretariat Records Officer only (The Main Records Unit for filing purpose)
- In cases of investigations, access may need to be extended to authorised investigating officers from other organisations, e.g. Audit or Police.

Access restrictions are normally made for an entire file or a class of files. Often, the nature of a class of files makes the need for access restriction obvious – e.g. Personal Files. For these cases, the department should make a list for access restriction on the entire class of records. Any new file opened under this class of records will then automatically fall under the same access restriction. If an access restriction is made for a whole file, any new document put on this file is under the same access restriction.

Access restrictions for files or classes of records need to be made in writing with a brief explanation for the reason. A register of restricted files has to be kept.

Files which are access restricted need to be marked clearly on their cover and in the records management system as restricted, and should contain handling instructions written on the inside of the front cover.

Files with access restrictions need to be stored in a safe location away from unauthorised access. If the work area of a records staff does not have a lockable storage, the file needs to be returned every day after work to the records unit for safekeeping. Records staff (that the file belongs to) is responsible for following up that this is done.

Access to Personal File:

No person shall have access to the personal files, including the staff member's own personal file, without written permission of the Vice-Chancellor to a specified person to access the whole or part thereof, and upon application to the Vice-Chancellor, the written delegated authority to a specified employee (e.g. Manger, Personnel and Personnel staff), a specific lawful order directing the University to provide part or whole of the member's personal file.

A copy of the written order shall be attached to the member's file.

A record shall be maintained of any documents taken by lawful order, or any documents photocopied from the staff member's personal file.

Security of personal files shall be maintained at all times. Under no circumstances shall a personal file leave the area designated for the storage of the files. All information contained in personal files is to be treated as confidential and must not be divulged.

Outgoing Confidential Correspondence:

For outgoing correspondence that needs to be access restricted, the author writing the document is responsible for making the restriction. The access restriction has to be clearly marked on the document, on top and bottom of each sheet.

Confidential mail should be sent under double cover. The outer envelope must not bear any classification nor should it be sealed. The sealed inner envelope is marked with the access restriction.

Incoming Confidential Correspondence:

Mail marked as "confidential" delivered to the NUS is official office mail. It therefore has to be registered and referred to Chancellery/appropriate person as soon as possible (1-2hours max).

All incoming confidential mail should be registered by Executive Secretariat Assistant/secretary/assistant, who is responsible for the safe delivery of the document to the authorised recipient.

The recipient needs to direct the records officer as to whether the document needs to be filed under an access restriction.

B. Making Access Restrictions for Records to be Transferred to Central Records Unit

Every section/department needs to make a decision on all records they transfer to the Central Records Unit regarding any access restrictions, based on the above mentioned principles. If an access restriction is made, this decision must be documented and formally submitted to EXECUTIVE SECRETARIAT RECORDS OFFICER, using the *Transfer Agreement Form – Access Restriction*.

All records without a formal access restriction coming to the Central Records Unit are considered open to the public.

GUIDELINE 3:

FILE CREATION, CLASSIFICATION, TITLING AND REGISTRATION

This is a guideline to be used when creating new files

FILE CREATION

Search for an existing file - When a document comes in for filing, the records staff must decide whether an appropriate file already exists. Only if no suitable file exists, a new file will need to be created and a title allocated consulting the NUS Classification Scheme.

Do not open new files if you have no documents to go on it - No new files should be opened before there is documents to go on it. Opening new files in the expectation of future documents leads to waste of effort, waste of valuable file covers and, most damaging of all, confusion in the file system.

Use file covers which meet required standards - All file covers used for registered files need to be made of plastic coated cardboard with plastic file fasteners attached. Every paper has to be attached using the fastener. Brands of suitable covers available in local stationery shops in Samoa include 'Dalton Files' and 'Coda Files'. Arch-lever binders, manila folders and any files with metal fasteners or pins do not meet the required standards. They should only be used for keeping documents together before filing and for reference materials.

Do not put non-record materials on registered files - Not all papers need to be placed on registered files. Do not put duplicates, working drafts and publications of other agencies in a file, unless they contain information concerning the file matter which is important and unique. Refer to *Guideline 13 – Normal Administrative Practice* for guidelines. If you need to keep non-file reference material, put them in your own library collection and discard them if they are no longer used.

Do not put unsuitable material on paper files - Do not file overhead transparencies or thermal fax paper – photocopy and file instead. Remove adhesive tape and any metal objects like paper clips and bulldog clips, and plastic covers or sheets (they can lift the print off paper). Post-it notes can fall off, therefore encourage making file notes on the back of documents instead. Remove document bindings, e.g. spiral binders, before placing it on the file, because it makes the file bulky and can break the cover.

File records in date order on the file - Always file according to date of document with the most recent being the top document on the file. This means that you have to file a document which you have received late in order of the date range which may result in the document not being placed on top.

Do not overfill the file cover - Close a file and make a new part once the file gets over three centimetres thick.

FILE CLASSIFICATION & LABELLING

Always use the NUS Classification Scheme – The NUS Classification Scheme is a system must be used when title the files. Titling files according to the approved NUS Classification Scheme makes it easier to search for a file and makes records easier to sentence for disposal or retention. This classification also aids in consistent titling, as you are using standard terms for describing the content.

Determine any access restrictions to a file - Some files will need to be restricted with access limited to certain authorised people. File covers need to be marked clearly if an access restriction is given to the file. Refer to the *Code of Best Practice, Guideline 2 – Access* for guidelines on when and how to give access restrictions to public records.

Relate to any relevant files - If a file is related to another file or if there are any previous parts, note these file numbers and part numbers on the cover of the file being created. Make sure to also update the covers of the files that you are relating this new file to. You may also need to relate to objects that cannot fit on the file (e.g. maps, videos, CDs, discs).

Label file covers with all necessary information –

The following information needs to be written on file covers:

- Location code – shows where the file is located (room/office name code+ book shelve or cabinet number, e.g. DFOS**A01** – FOS Dean's office-A cabinet-01 shelve)
- Number and Name of the main category from the NUS Classification Scheme (e.g. 1.Meetings)
- Number and Name of the subcategory in the NUS Classification Scheme (e.g. 1.1. Internal Meeting)
- CARS Code if necessary
- The name of the file (e.g. 1.1.6. Senate Meeting)
- The date (can be from one year to another year)
- access restrictions (if any)
- specify ACTIVE/TEMPORARY/ARCHIVE
- destruction year
- the electronic file code
- the table of content on the inside of the folder
- file's cardboard (on back cover – for more details, refer to *Guideline 5 – Managing Current Files*).

When the shelves are labelled, different colours should be used. The labels of the folders will have the same colour than the shelves where they will be stored, will be more easy to retrieve.

FILE TITLING

File titles should accurately describe the contents of the file - If the title does not reflect the contents of the file, it is difficult to locate records that are being searched for. The title must also assist users to add new documents to the correct file classification.

Be consistent - If files on similar things are titled similarly, it makes them easier to retrieve. Make sure that you use a name following the NUS Classification Scheme this will help to classify them more easy.

Do not use acronyms, abbreviations or jargon - Some acronyms or abbreviations can have different meanings at different times which is why they should not be used as a rule. There are however circumstances where the use of acronyms or abbreviations is appropriate (e.g. "UNESCO" as the organisation is commonly referred to as UNESCO). You should keep a list of which terms are approved for use and keep them in the NUS Manual and Procedures.

Do not change a file title unless absolutely necessary - When adding new papers to a file, take care that the file title continues to reflect the contents accurately. At the same time, do not change the title of a file unless it is absolutely necessary. Users become familiar with titles and so there can be confusion if you do change it. If necessary, create new files for new papers and make cross-references to the files containing earlier related papers.

FILE REGISTRATION

All files must have unique reference numbers - The reference number for a file should be constructed in accordance with the NUS file Classification Scheme.

GUIDELINE 4: MANAGING CORRESPONDENCE

This guideline refers to the registration and processing

of incoming and outgoing mail, and of internal correspondence.

All official correspondence of the NUS needs to be captured in the NUS recordkeeping system. Therefore, all correspondence needs to be registered and filed.

Incoming Correspondence

It is important that all incoming correspondence is handled efficiently so it can be actioned as soon as possible. Some will come through the mail, some by hand and some by fax or email. These are the steps that need to be considered when managing incoming correspondence.

Opening mail - All mail that are opened should be date stamped as soon as it is received. All staff should be aware that all mail to the NUS address is considered official mail and therefore will be opened by the Executive Officer or Assistant Executive Officer (Secretary if the letter will go directly to one of the NUS sections/departments), even if it is addressed to an individual. Confidential mail and mail marked "Personal" should not be opened. If a letter turns out to be a private matter not relating to NUS work, it should then be given to the individual without date stamp or registration. For general guidelines, see *Guideline 2 - Access*.

Cheques received in the mail should be registered separately and forwarded to your accounts section.

Registering incoming correspondence – Once received, incoming correspondence needs to be stamped with date and time received, and registered into "Incoming Mail Registry". Registered mail must be referred to Chancellery/Secretary/Assistant as soon as possible (1-2hours max). All incoming mail directed to the Chancellery floor should be registered by Executive Secretariat Assistant, who is responsible for the safe delivery of the document to the recipient. The other incoming mail directed to the other NUS sections/department must also be registered by the responsible staff member in the section/department (secretary, assistant, etc)

File correspondence and forward to EXECUTIVE SECRETARIAT RECORDS OFFICER – The new incoming correspondence needs to be attached to the appropriate file. If there is no suitable file, a new file needs to be created following the NUS File Classification Scheme.

The correspondence should be actioned while it is attached to its file, because this file contains the background information necessary for decision making. It also prevents the loss of documents, as a file is easier to locate than an unattached sheet of paper.

There may also be situations where more than one person needs to receive the correspondence; the original then still should be placed on the file after the document is registered, and copies provided with a file reference number, so all other action officers know which file to refer to.

The Assistant Executive Officer is responsible for determining which division the correspondence is forwarded to for action at the Chancellery floor. If the VC is actioning a correspondence themselves, the document should still be returned to AEO so the relating file can be retrieved or created. Ensure the procedures for documenting file movements are followed in all cases (Refer to *Guideline 5 – Managing Current Files*).

Internal Correspondence

Internal correspondence includes internal memos and directives. Internal correspondence relating to University work needs to be registered, filed and managed as official records. Internal correspondence relating to University's work therefore should be registered in an Internal Correspondence Register and placed in the relating registered file. If the memo is distributed to more than one person, the original has to be attached to the file.

Outgoing Correspondence

A copy of all correspondence that is sent out by the University needs to be copied, registered and filed on the appropriate file. All mail delivered needs to be recorded in the Outgoing Mail Registry and signed off by the recipient. The information that needs to be recorded in the Outgoing Mail Registry includes date letter despatched; where sent (ministry/division/organisation); name and signature of receiving officer and date.

GUIDELINE 5: MANAGING CURRENT FILES AND CLOSING FILES

This guideline refers mainly to the management of existing paper files.

For the specific issues relating to the management of electronic records, see

Guideline 7 – Managing Electronic Records.

For the creation and registration of new files, refer to

Guideline 3 – File Creation, Classification, Titling and Registration.

All files containing official records must be registered into the records management system of the NUS.

Ideally the Central Records Unit will be responsible for the custody of all NUS files it has registered. If this is not possible due to the NUS sections that store their own files, then the section who regularly require the files may be given these files to look after for as long as they are in current use. **It is important to note that these files are still part of the Central Records Unit, that they are registered under NUS Records Management System and that all correspondence going to them is registered under this system. Therefore, sections or senior management should not create or store unregistered files containing official records.**

It is also not recommended to keep duplicate copies of registered files because it is very difficult to make sure that both copies will contain all records in identical form *(e.g. correspondence may be received by the Main Office without the division being aware of it)*. It also creates much waste and makes organised disposal difficult.

Keep records safe - Keep records in a safe location following the guideline *Guideline 10 – Records Storage Rooms*. Make sure that shelving space remains adequate even when more files are created – do not squeeze more files into full shelves or filing cabinets. Closed files which are not used frequently any more should be stored in boxes. Current files in standard file covers should be placed on shelving using metal file racks, with coding facing outwards. Filing cabinets can be used for confidential files.

Do not remove papers from files - Papers should only be removed from files if they have been misfiled or were placed on an incorrect file. They should not be removed under any other circumstance. If individual papers are needed from files, then make a photocopy of it but do not remove them from the file.

Cross-referencing documents on files - If a single letter or other item of correspondence relates to more than one file it should be photocopied and the original placed on the file for which it has most relevance. Place the photocopies on the other files to which the letter relates. On the original letter note the file code on which additional copies have been placed. Similarly, note the location of the original on each copy placed on other files.

Issuing Files - Before issuing a file to a user, make sure the user is authorised to view this file.

Record file movements - The location of a file always needs to be known. Each time a file is moved, this action must be recorded. File movements are monitored in a number of ways: on file transit cards, on transit tables that appear on file covers, and through regular file audits, which are described below.

File Transit Cards and File Out Cards **-** Each time a file is issued to a user, the user's name and date must be noted by records staff on the **file transit card** or file transit sheet. Also record the date when the file is returned to the records room - do not cross off or delete the user's name from the transit card when the file has been returned, because this information is needed for a complete record who had the file at any time. There are two options how to store transit cards:

1. The file transit card is always kept in the **file transit folder** or file transit book. To mark where the file has been removed from the shelf, a blank file out card is kept in the shelf in the position of the file. This option also makes the task of file auditing (see below) easier.

2. The file transit card is kept in the file when on the shelf, and is removed from the file and placed on its position on the shelf when the file is taken out. This method is not particularly recommended, as experience has shown that transit cards can easily get lost between files on the shelf.

Transit Table - Each file movement must also be recorded on the **transit table** or transit ladder on the front of the file cover. This records the same information that appears on the file transit card. Transit tables provide a record of all persons who have handled any particular file.

File Audit - In order to confirm the location of files, records staff should carry out a regular audit of every file outside the records room. Records staff must visit every action officer to list all the files held by that officer, and then check the information on this list against that in the transit book to ensure that the up-to-date location of each file is correctly recorded.

Tracing missing files - If a file is missing, proceed as follows:

a. contact the action officer to whom the file was last recorded in the file's transit card and ask him or her to trace it.
b. If this fails, check the records room if the file has been misfiled or returned without the transit card being updated.
c. If you do not find it, circulate a note to all staff of the NUS asking them to check whether they have the file.
d. If the file still cannot be found, a special search must be initiated. The search must be repeated several times if necessary.

Report Irregularities concerning Files - As soon as the records staff learn that a file is missing and may be lost, they must write the words 'missing file' on the relevant transit card. A list of missing files should be maintained, periodic searches carried out and a record kept of the areas searched. If a file remains missing, or any other irregularity (e.g. tampering with documents) is suspected, a written report has to be submitted by the records officer to the EXECUTIVE SECRETARIAT RECORDS OFFICER. Make sure a copy of this report goes on

file. Depending on the seriousness of the incident, the Vice Chancelor will be informed, who in turn may report this irregularity to PSC, Audit, Ministry of Finance and any other relevant bodies, in accordance with PSC procedures.

Temporary Files - If action on a topic covered by a missing file continues, open a temporary file. This should only be done if absolutely necessary. A temporary file is opened in the same way as a normal file. It is given the same number as the missing file and its existence is recorded in the normal way. If available, temporary file covers should be used. If temporary file covers are unavailable, a standard file cover should be used but must be boldly marked with the word 'TEMPORARY'. All relevant record sheets should be similarly marked.

When the original file is found, all papers on the temporary file must be transferred to the original file (in proper date sequence). Mark the front cover of the temporary file with the date that the original was found. The printed area and transit table of the temporary file cover should then be cut away and placed on the original file. The temporary file's transit card must similarly be marked with the date that the original was found and then struck through, but retained in the same place in the respective books. Also amend the transit card for the original file and update the list of missing files to show that the file has been found.

Returning files – the files should be returned to their main location as soon as finished with them. It is the responsibility of the records staff to ensure that this is done.

Closing files - Ensure that files are closed as soon as they become either three centimetres thick or five years old, whichever is the sooner. Do not add further correspondence to files that are closed, except it is a document which should have gone on this file and is filed belatedly. The method of closing a file is to write the word 'CLOSED' in large and clear letters across the front cover, together with the date the file was closed. The file transit card must be marked to show that the file has been closed. The date when this was done is also recorded. Mark the volume number of the closed file volume on all relevant indexes and registers.

If it is necessary for action to be continued on a topic covered in a file that has been closed, a new file part should be opened. The existence of the new part must be noted on the transit card for the closed part. Also add a special coloured paper on top of the closed file with information about its date range and the reference to the new file part. The new file part should carry a note explaining that the previous part has been closed and giving its reference.

Custody of closed files: Although no new action may be taken on a closed file, and no new papers added, closed files should be kept available in the records room (or in a nearby file storage area) for a period of time so that users may easily refer to them. The retention period is specified in the NUS Records Retention Schedule (*Guideline 12 – Sentencing Records* for details).

GUIDELINE 6: NUS RECORDS MANAGEMENT SYSTEM

This guideline lists the requirements for the NUS Records Management System.

The NUS Records Management System is a system that controls records and stores information about them. It is paper based system, using NUS File Classification Scheme, register books etc., and also an electronic system such as a computer database, which collects and manages information about the records.

The NUS Records Management Systems

1. is able to routinely capture and manage all NUS records
2. retain authentic records as long as needed, by protecting them from unauthorised access, alteration or destruction through appropriate security measures and back-up; electronic systems, has an online back-up and an extra hard drive available for back-up
3. provides ready access to all relevant records and related metadata (= "data describing a record" can be found in NUS Records Retention Schedule)
4. is capable of continuous and regular operation in accordance with the NUS records management procedures.

Training

All the deans, managers, directors and heads of departments must make available and guide their staff to attends the seminars, trainings, meetings and workshops organised by Central Records Unit so that the NUS Records Management System is correctly used and retrieval of the documents will be easy and fast.

NUS Records Management Systems

Includes:

- NUS File Classification Scheme
- NUS Records Management Policy
- NUS Records Retention Schedule
- NUS Records Manual and Procedures

Electronic Records Management Systems

One of the main benefits of having an electronic records management system is that is possible to search on **any** recorded type of information about a document or file. Another benefit of an electronic records system is that it enforces the methodical registration of records.

GUIDELINE 7: MANAGING ELECTRONIC RECORDS

Electronic records are records that have been created by a computer. They present special challenges to recordkeeping. This guideline provides basic advice on the creation, filing and preservation of electronic records.

NUS electronic records system

The NUS electronic system follows the NUS Classification Scheme. All the 16 main classification categories and their sub classifications have a short name made out or 3 or maximum 4 letters. These can be found in the list of the NUS Classification Scheme. These letters helps to compose the electronic name of the files that will tell its place in the NUS Classification Scheme. In the NUS Classification Scheme can be found in a column sample of the short name of the electronic naming.

Documents need to be saved under a title which clearly identifies the content of the file, the date and the location in the NUS Classification Scheme. The name must include the 3-4 letter name that shows the location in the NUS Classification Scheme, the date (year/month/day) and a Short Title or a name that will describe the contain of the file.

Each main folder of the 16 main classification categories will have an excel register with a list of files and hyperlinks to the documents in the folder. In this register can be added more information about the documents. (E.g. Document title, description, institution or person involved, date of the document, date of the signature, date when the document was read, how many pages the document has, the destruction/transfer year, person that received the document, person that filed the document, etc.) The order of the documents in the register can be by date, by document title or by Institution/Person/Company.

Example: The General & Casual Staff Manual that was created in march 2015 could be called:

"PMP-PLM-GSM-2015-03 NUS General Staff Manual"

This name is telling us that the file is under:

7. Policy Manual and Procedures (PMP)

7.1 Policies and Manuals (PLM)

7.1.1. General Staff Manual NUS (GSM)

And was created in march 2015

If there are different versions of a document, the title needs to identify the version (e.g. *draft*, *final, Ver.2.1*).

If another type of directory is neded to be created, it has to be established centrally in cooperation with the central records office. All NUS sections should follow the NUS Classification Scheme.

The controlled terms used by the records office (found in NUS Classification Scheme) can serve as the basis for naming directories and files in a consistent way.

Train staff - All staff in the NUS who use a computer need to be aware of the rules guiding the naming of electronic documents and the directory structure, and to attend to the trainings provided by central records office in how to use it correctly.

Manage shared folders in conjunction with your recordkeeping system

Shared folders – either network drives or 'public' folders in some email environments – are increasingly being used by most NUS sections. There are many good reasons for this, but there are some ***risks*** which need to be considered:

a. It is easy to develop a confused, uncontrolled hierarchy of folders and document titles.
b. Security settings that permit users to save documents to the folder also may give users the ability to inadvertently delete or alter a document.
c. Documents that relate to one activity may be stored in different locations (either within the shared folder, or in other systems), which makes it hard to find all versions or relating documents.
d. Limited capacity of information technology infrastructure and a lack of authorised disposal procedures may mean that there is pressure to destroy documents while they are still useful.

Shared folders are a useful tool, if you ***ensure that proper records are kept*** as well. Some of the ways this can be done include the following:

a. Provide links between the shared folder and the NUS Classification Scheme.

b. All users must create proper file titles and using the proper folders.

c. Ensure that copies of all approved or final versions of documents are placed into your recordkeeping system, i.e. registered paper files, and that all staff are aware that the 'official' version of the document should be obtained from the registered paper file.

d. Ensure that draft documents are clearly labelled as drafts, and that they are all filed under the proper folder. Draft versions normally should be removed from the shared folder after the final version is completed. Draft documents needed as evidence for important changes should also be filed in the registered paper file.

e. Remove out of date documents from the shared folders and correct misfiling on a regular basis.

f. We have security measures that limit the ability of most users to create folders and delete or amend documents.

Back up all electronic records

Dependable backup procedures are needed to protect electronic documents from loss and corruption. Individual hard drives on personal computers (PCs) are not backed up via the regular network backup procedures and must be backed up regularly by users on line on Google Drive under NUS account.

Use discs correctly

Discs may be used to store documents with a very low reference rate or to back up individual hard drives. In addition, they are used to transport documents in the absence of network access. Private memory sticks/USP/pen drives etc. should only be used to transport documents, but not for storage.

Use appropriate directory structure - The directory structure of discs should be the same as NUS Classification Scheme.

Label discs and tapes - All electronic media items must be labelled. External labels on disc covers should include the name of the originating office, the title of the document or document folder and the date range (i.e. dates of the oldest and the most recent document). They should indicate the software required to read the disc (e.g. "Microsoft Word 2002"). Access restrictions should be indicated on the label when applicable. A printout of the document index should be stored with the discs for retrieval purposes. Discs should be filed systematically, following the NUS Classification Scheme as well.

Handle electronic media carefully – Electronic media needs special handling if electronic records are to be preserved for more than a short time. File custodians should know which files are permanent, what is to be done with them and when.

The following are general maintenance suggestions.

a. Backup files onto discs often – preferably after every update. An system backups should be perform periodic. Ideally, backups should be kept off site.
b. Keep disc and tape drives clean.
c. Keep discs and tapes away from strong electrical or magnetic fields, e.g. from the top of your computer hard drive.
d. Do not touch the recording surfaces of floppy discs and tapes.
e. Do not allow unauthorised persons (e.g. children of staff) to have access to the computer. Even people with good intentions can enter commands that will delete files or reformat hard disks.
f. Keep food and drink away from storage media as well as equipment.
g. Store discs and tapes in a vertical position in a storage container (for example a disc box).
h. Store discs in a cool, dry environment away from sunlight.
i. When upgrading to a new software or new system, migrate all electronic records required – including your archival records – to the new system. This may require systematic updating of existing backup tapes.

Special Advice for Facilities Storing Permanent Electronic Records:

Data processing facilities storing magnetic tapes containing permanent records need to take account of the following points:

1. Store magnetic tapes in a dust-free environment at a constant temperature between 18-20 degrees Celsius and at a constant humidity between 35 and 45 percent.
2. Read annually a statistical sample of all permanent and unscheduled data sets stored on magnetic tape to detect any loss of data.
3. Periodically rewind tapes at constant tension, at normal tape speed.
4. Copy data on the tapes to new or re-certified tapes at least once every ten years or more frequently when necessary to prevent the physical loss of data or technological obsolescence of the medium.

GUIDELINE 8: MANAGING EMAIL

This guideline provides instructions on managing email as a public record.

The use of email is an important tool for NUS to conduct business. Previously, information was communicated and preserved in paper form. Now, it is often part of an email message, in electronic form.

Email is a record

As emails are made or received by almost all NUS staff as part of the jobs they do in NUS they are definitely considered to be public records.

Records can be made up of one or more documents. This is often true of emails which may be made up of an email plus attachments. In this case the record would consist of both the email itself and its attachment(s).

Types of Email:

1. **Personal email** is email which relates to a private or personal matter and has nothing to do with the business of the NUS. It therefore is not a public record. Examples of personal email include email dealing with topics such as lunch invitations, family matters or sharing jokes or prayers. Personal email can be destroyed as soon as staff no longer requires the email.

Note: If an email incorporates personal and work-related information, then the email is a public record.

2. **Facilitative email** is email which facilitates NUS business but which does not need to be retained for business purposes. Examples of this type of email include notices of meetings, newsletters, advertising material and any other publicly available material, and internal work-related email received by "carbon copy" (cc) or "blind carbon copy" (bcc).

Facilitative email can be destroyed as part of normal administrative practice - refer to *Guideline 13 – Normal Administrative Practice.*

3. **Corporate Email** forms part of the public record. It is email that documents the business activities of the NUS. Examples of emails which form part of the public record include communications between staff in which a formal approval is recorded, directions for an important course of action, and business correspondence received from outside the NUS.

Corporate email must be retained for as long as is determined in the NUS Retention Schedule.

Managing Corporate Email as a Public Record

Email systems are used to create, send and receive email messages e.g. *Outlook, Yahoo, Hotmail*. These systems however do not store or manage emails well. This is especially true for internet based email service providers like *Yahoo* and *Hotmail* where email is regularly purged when mail

boxes become too large or cannot be accessed any more when staff members leave. All corporate email should be conducted through your NUS email address.

With all email systems, there is a danger that important corporate records may be lost if email is not properly managed. A strategy therefore has to be put in place to reduce this risk.

The following requirements for managing corporate email as public records has to meet:

1. Emails should be accessible – Authorised staff should be able to read emails which are relevant to their business.

2. Emails should not be able to be altered – Emails should not be able to be altered (or alteration should only happen in an authorised and detectable fashion), otherwise they may not be considered reliable evidence.

3. Emails should be correctly filed - Emails should be classified and filed in such a way that they are related to other documents (paper or electronic) on the same subject, so that they can be found easily and linked to all other relevant information.

4. Emails should be readable for the long term – Emails with long term value need to be preserved in a way that they are readable as long as prescribed, even after a change of computer operating systems or software. One way to do this is to archive the old e-mails and save that archive online together with other important NUS documents.

The practical consequences of these requirements and the nature of electronic records are that there are only two acceptable options: Printing the email as paper copy for file, or using an electronic document and NUS Records Management System which meets international standards.

If electronic versions of the corporate emails and other electronic documents need to be kept, you should save them in a structured way following the NUS Classification Scheme by changing the name using the proper naming to fit the Scheme and save the document in the proper folder. refer to *Guideline 7 – Managing Electronic Records* for more information. This means that corporate emails will be available for others to read and will be located with other relevant records.

NUS Records Management Systems

NUS Records Management Systems is an information system which capture, maintain and provide access to electronic records over time. It includes: The File Classification Scheme, Records Management Policy, Records Retention Schedule and the Records Manual and Procedures. All ensure that the content and metadata (i.e. data about the document) of electronic records are managed so that the records are preserved and remain accessible.

GUIDELINE 9: BOXING AND LISTING

This guideline gives instructions on the proper storage of closed files.

Sorting records – Records need to be sorted and put into an order before they are boxed up. This guideline is for records which have already been identified for storage – for the identification process, refer to *Guideline 12 – Sentencing Records* for instructions.

First separate the files according to NUS Classification Scheme. Within each of the 16 categories, sort the records first according to the disposal due date *(e.g. put together all records which are to be destroyed in 2010)*.

Then put the records in order by subcategories within the 16 main categories and by date range. Box and list according to this order.

Use appropriate boxes – All closed files have to be stored in boxes.

All ARCHIVED (PERMANENT) records need to be stored in boxes that are specifically made to store records and which come with the lid attached. These boxes have to be small enough that they can be lifted and be carried easily by one person who is not a weightlifter. The purchase of these boxes is the responsibility of your section, however the Main Records Office can provide details of suppliers. Contact the Executive Secretariat Records Officer for advice for the packing and storage of oversized items such as large ledgers & rolled plans which do not fit in small boxes.

Packing records in boxes – All records have to be clean and free of any insects before being placed into the box. Loose papers must be placed into labelled manila folders before they are placed into boxes. For the packing of permanent records refer to *Guideline 15 – Transferring Records* for further guidelines. Place files with spines down into the boxes so they can be easily lifted out. Pack boxes from left to right, with lid attached to your right-hand side. Remember to keep files in their original order as also indicated in box lists. Boxes should not be too tightly packed so records can be lifted easily out of the box. Close the box lids but do not tape them.

List and Label boxes – Every box needs to be numbered and listed to make searching for records easy. List the contents of each box. These box lists are very important tools for finding records.

The following fields need to be on the box list:

- Name from one of the 16 Main Category that the files belonging to.
- Location of storage room
- Location of box in the storage room e.g. shelf number
- Box number (must be unique)
- File name like is in the electronic copy
- Volume number if existing

- File title, or description of records if there is no clear title
- Date range (from date of oldest document, to the date of the latest document)
- Disposal action (destruction due date)

You need to keep one complete list set in your office, and another list set in the storage room. Make sure you update both copies when more boxes are added to the room or transferred. It is also useful to place a copy of a box list in the box it refers to. Label and list boxes as you go along. Label every box on the narrow end of the box with the lid attached to your right-hand side. There are special labels for permanent records which are eventually going to be transferred to Records Main Office. These are provided by the Executive Secretariat Records Officer (refer to *Guideline15 – Transferring Records* for details). Every box needs a unique number which refers to the box content list. This number will be given by the Executive Secretariat Records Officer before the box is transferred. Other useful information for the label could be the Section/Department name, the category from the Records Classification Scheme date range, and destruction due date.

Know where your boxes are - The location of the boxes in the room also needs to be recorded using the location field on the box list, a labelled floor plan and corresponding signs on the shelving.

GUIDELINE 10: RECORDS STORAGE ROOMS

This guideline sets out minimum storage requirements of records held by NUS

This includes all storage areas used to store non-current records (*e.g. closed files).*

Keep room secure - Access to rooms has to be restricted to authorised staff only (*e.g. Executive Secretariat Records Officer, HOD, Deans, Managers, Directors*)**.** The room should be kept locked at all times when not being used by records staff.

Safe location - The room has to be situated in a safe area, away from potential hazards such as rising sea water, leaking roofs, toilets, food, or open public areas.

Keep room clean - The room needs to be kept clean, with all rubbish and dust removed regularly. Rooms have to be checked regularly for any signs of insects, rats, mice or other pests. If any signs are detected, pest control measures have to be undertaken immediately. No food or drinks of any kind may enter the room.

Keep sunlight out of room - Any windows in the room should be blocked. Sunlight is extremely damaging to records and therefore should be kept out where possible.

Keep water out of room - No water can be allowed to enter the room. No piping or sinks should be in records storage rooms.

Maintain air conditioners - Air conditioners need to be maintained with repairs undertaken as soon as possible if broken**.** Should the air conditioner be leaking water, it has to be turned off immediately and kept switched off until it is repaired.

Use Archive Boxes for non-current records - All non-current records (e.g. closed files) should be kept in archive boxes. These boxes should be small enough that they can be lifted and carried easily. Refer to *Guideline 9 – Boxing and Listing* for guidelines on how to store records in boxes.

Use Shelving - All records have to be kept off the floor. All records should be stored on metal shelves or commercial archives shelves made of treated wood. As an interim solution before enough shelving is available, boxes can be stacked on clean pallets in a pyramid formation like brickwork. If they were stacked straight on top of each other, the boxes could easily collapse under the pressure – this method is therefore not recommended.

If the type of shelving requires lifting records from high levels, a secure ladder or a special safety stool has to be provided, to allow safe retrieval of boxes.

Know where your records are - All boxes need to be labelled and listed so that there is control and the records can be retrieved when required. A complete, regularly updated box list needs to be kept in the storage room. A copy of this list needs to be stored as backup at different location. Refer to the *Guideline 9 - Boxing and Listing* for further information. The location of the boxes in the room also needs to be recorded using the location field on the box list, a labelled floor plan and corresponding signs on the shelving.

Records Only - Only records should be stored in designated records rooms. All other items such as office equipment waiting for write off, empty bottles, car parts including tyres, matts, Christmas decorations, dirt, machinery etc. do not belong in a records storage room and must be stored in a different location.

GUIDELINE 11: EMERGENCY PLANNING

This guideline advises on ways to protect public records from disasters,

and to minimise damage to them in an emergency.

Samoa as a nation is threatened by natural disasters, such as cyclones and tsunami waves. Additionally, many records storage areas are at risk of being affected by other events which can cause damage to records, such as flooding, a leaking roof and fire. Electronic records are also threatened by other types of damage, such as computer virus, system breakdown etc. It is our duty to keep these risks at a minimum level, and in the case of any disaster, to minimise the effect it will have on the records and the information contained in them.

Take preventative measures - Minimise hazards in records storage areas e.g. by repairing leaking roofs, storing all records off the ground, maintaining air-conditioners, removing rubbish, managing pest control, and keeping hazardous material away, including maintaining a strict non-smoking policy around records.

Establish the vital records of your Section/Department – Vital records are those records which are most necessary to fulfil the section's/department functions, and especially those which will be very important for a quick response to a nationwide disaster. These records may not always be permanent records, but are essential for the present operations of the section/department. Examples for such records would be course reader for the faculties, infrastructure plans for the planning unit, the financial management system, staff salaries and entitlements, etc. Vital records also include your records management systems, e.g. file index lists, so that you can determine if any files were destroyed.

Make Back-up Copies – In most cases, a back-up copy of records will be the most useful tool to enable quick disaster recovery and continued operation of your section/department. Therefore, back-up copies of vital records should be made, and of any other record, especially those which are considered permanent. Back-up copies of vital paper records could be photocopies or digital scans. For more information about back-up of electronic records, refer to *Guideline 8 – Managing Electronic Records*. Back-up copies should be stored off site at a different location to the original record. Some Samoan back-up copies are actually stored off island. If the back-up is in electronic form, regular checks need to be made to ensure the information can still be retrieved and read.

THE FIRST PRIORITY OF ANY EMERGENCY RESPONSE IS THE SAFETY OF STAFF AND THE PUBLIC.

Provide Emergency Response Supplies – Every NUS Section/department has to have a kit of equipment to respond to emergencies.

This set must include:

- Flashlights with spare batteries
- First Aid kit
- Plastic sheeting
- Plastic bags
- Mop and bucket
- Protective gear, such as dust masks, gloves and aprons
- Washing line and pegs (to dry files)
- Marking pens, pencils and writing pads
- Spare file boxes
- Manila folders
- Masking tape
- String
- Scissors
- Absorbent paper and paper towels

This tool kit needs to be kept in a closed, sealed container which may only be opened for emergency response. Another first aid kit should be provided outside the container for injuries that occur under regular work conditions.

GUIDELINE 12: SENTENCING RECORDS

Sentencing is the process of selecting the appropriate disposal action for records.

It involves classify a record using the NUS Classification Scheme and check in the NUS Records Retention Schedule.

NUS Records Retention Schedule

In order to determine how long, you need to retain certain types of records and whether they can be eventually destroyed or kept as archive, you will need to use a records retention schedule. A schedule lists classes of records, sorted according to functions and activities, and states the disposal action i.e. how long the various classes of records need to be retained for. The records will either need to be kept for a certain number of years before they can be destroyed or transferred to the Main Archives Office as permanent records.

When should sentencing be done?

Ideally sentencing should be done at the creation of a record. This means that records can be treated according to their value and preserved for only as long as they are needed. This is particularly important for electronic records. However, disposal action can only be taken after a file is closed and is not the subject of any legal proceedings or investigations.

Guidelines for Sentencing & Disposal Actions:

Note: Because of the need to interpret retention schedules when identifying and classifying records it is strongly recommended that sentencing is carried out with the help of the Executive Secretariat Records Officer.

a. All documents that can be destroyed by **Normal Administrative Practice** (Refer *Guideline 13 – Normal Administrative Practice* for details) should be separated from those records that will need to be sentenced using the NUS Records Retention Schedule. It is easier to identify records series once this initial sorting has taken place.
b. **Separate all records created before 1966**. Contact the Executive Secretariat Records Officer for a decision on these records. They cannot be sentenced using the presently existing records retention schedules.
c. **Use the NUS Records Retention Schedule** for the records you are about to sentence.
d. Make sure you are using **correct the NUS Records Retention Schedule** for the records you are about to sentence. Contact Executive Secretariat Records Officer if you require assistance.
e. **Never remove documents from files** as this may compromise the integrity of the file. Sentence the entire file as it exists.
f. Be sure to first **check the contents of every file** and not just the file titles. The file title will provide a clue as to what to expect on the file but you need to check the contents to be certain.
g. If you cannot find a disposal class that fits a file, put it aside or ask the Executive Secretariat Records Officer to review it.
h. If you find a file that fits more than one disposal class, **always use the class with the longest retention period.** This will be the case for example if a file relates to more

than one activity. Files from the category 'correspondence' usually belong to this category.

i. Some files have more than one part to them. Generally, you can sentence each part as a separate item and either destroy or keep them according to the instructions of the Retention Schedule. However, it may be that the parts you plan to destroy have information that is needed to understand the parts that will survive. Use your own judgement.

j. **Document all decisions.** Make sure to update your control file record (i.e. file list, database, index cards, registers) to show what has happened to the file (i.e. destroyed or transferred to Main Records Room). Use the approved form for records destruction (*Authorisation & Notification of Records Destruction*) and the template prescribed for transfer of records to the Main Records Room.

k. Closed files identified for further retention – either temporary or permanent - should be placed in boxes which need to be numbered and a contents list created. Where possible, files of similar types and review dates should be boxed together to aid the review process later. Files should be placed in their file number order within the boxes if possible – this makes retrieving files easier later. Boxes should not be too tightly packed. Refer to *Guideline 15 – Transferring Records* and *Boxing and Listing* for more information.

l. For destruction of records, follow the instructions given in *Guideline 14 – Records Destruction.*

GUIDELINE 13: NORMAL ADMINISTRATIVE PRACTICE

This guideline explains which documents can be destroyed without further authorisation as "Normal Administrative Practice" (NAP). Disposal of documents as NAP is only appropriate if no unique or valuable information will be lost.

To destroy a public record, a process of authorisation has to be followed. This may be through NUS Records Retention Schedule and authorisation by the Vice Chancellor of NUS (refer to *Guideline 12 – Sentencing Records* and *Guideline 14 - Records Destruction).*

However, some types of documents may not need to be placed within the recordkeeping system: They may only be required for a few hours or days, or they duplicate information recorded elsewhere. To cover these types of documents, the Normal Administrative Practice allows their destruction without further authorisation.

The following documents may be destroyed as Normal Administrative Practice and in accordance with this guideline.

- **Duplicates or extra copies of records** where the original or authorised copy is already filed in the recordkeeping system, and the duplicate is kept for reference purposes only (this also includes originals of thermal paper faxes or overhead transparencies, where a paper copy has been provided as authorised file copy);
- **Publications** such as magazines, sales catalogues, price lists, advertising brochures, newsletters, Christmas cards etc. **received by the office** (This does not include the material published by the office);
- **Library books and journals** (Note: books may be registered as assets and therefore may need to be written off);
- instruction **manuals for equipment** (destroy when equipment is disposed of);
- **Address** lists and changes of address notices;
- **Draft** documents in paper or electronic form
    - of which the final version is filed in the recordkeeping system
    - and which do not contain significant changes or annotations not included in the final document which need to be captured as evidence;
- **Working papers** including calculations, rough notes (e.g. of phone conversations and meetings), audio recordings of dictations and meetings, if the information contained in them has been entered into a final record filed in the recordkeeping system;
- **routine statistical and progress reports** compiled and duplicated in other reports;
- **calendars** and **appointment books**;
- **facilitative notes** e.g. spelling and editing corrections to documents, request for a file or an appointment;
- **stationery** including unused outdated versions of NUS letterhead and unused printed forms.
- **personal or facilitative Email –** for more information, refer to *Guideline 8 -Managing Email.*

Duplicates or drafts of confidential documents need to be destroyed in a way that they cannot be retrieved, e.g. by shredding.

GUIDELINE 14: RECORDS DESTRUCTION

This policy provides instructions on the

accountable and authorised destruction of NUS records.

Records destruction is the process of eliminating or deleting records beyond any possible reconstruction.

The following principles must be followed for authorised destruction of NUS records:

a. **Use NUS Records Retention Schedules** – The NUS Retention Schedule approved by VCC, must be consulted prior to any destruction taking place. The NUS Retention Schedule states how long to retain different classes of records for. Please refer to NUS Manual and Procedures, *Guideline 12 – Sentencing Records* for detailed guidelines.

b. **Ensure records are no longer needed** – While NUS Retention Schedules set a minimum period for retention, it is important to ensure that no one else in your section/department has any further need for the records.

c. **Obtain authorisation** – It is essential to obtain the proper authorisation to destroy any NUS records. The authorisation must be checked by Executive Secretariat Records Officer, Internal Audit and final signature from the VC and has to be documented by signing off on the form '*Authorisation & Notification of Records Destruction*'.

d. **Document the destruction** – The destruction of all records must be documented using the '*Authorisation & Notification of Records Destruction*' form. Make sure all records are listed. For files, list the titles and their file reference numbers. For other documents, such as vouchers, computer printouts, vehicle running sheets etc., write a short description and the range of running numbers. If you do not have enough space on the form, attach a list which needs to be initialled and sign on each page by the VC. The completed form needs to be forwarded to the Executive Secretariat Records Officer. The Internal audit should retain a copy for her records.

e. **Update records management system (filing lists)** – After a file has been destroyed it is essential to update your records management system or central filing list indicating that the file has been destroyed. You should also include the date it was destroyed and refer to the '*Authorisation and Notification of Records Destruction*' form for further details.

f. **Use appropriate methods of destruction** – Appropriate methods for destruction are irreversible and done in a way which is acceptable to environmental standards. The destruction of records should be conducted in a way that preserves the confidentiality of any information they contain. This means there is no risk of the information being recovered again.

- **Methods of destruction** - Methods of destruction of paper records available in Samoa are shredding or burning. For burning records, you need to obtain permission from the Ministry of Natural Resources and Environment, who will advise you on the location to be used. Make sure you remove all plastic material (spiral binders, arch lever files, plastic pockets etc.) prior to burning. Shredding is normally done for smaller quantities of paper, as it is a time-consuming process.
- Records stored on electronic / magnetic media should be erased and the media reformatted before being disposed of or re-used. Consult your IT officers for advice. (Note: Hard drives of personal computers and servers should always be reformatted before computers are disposed of.)

g. **Supervise the destruction** – Destruction of records has to be supervised by an authorised staff member (e.g. Records Officer, Internal Audit) to make sure everything is destroyed.

h. **Establish a regular schedule for destruction** – While records should not be destroyed when there is still a need for them, it is also important not to keep them longer than is necessary, to maximise storage capacity and retrieval efficiency. This task will be carrying out annually in November – December.

GUIDELINE 15: TRANSFERRING RECORDS

This guideline gives advice for the transfer of records to Main Records Room that have been identified as permanent and are no longer required for the current work of your section/department.

Interim Procedures

At present the Main Records Room has very limited storage space to receive records. This means that some of NUS section/department's record keepers will need to be the interim custodians of the archival records of their own section/department. It is therefore requested to follow all procedures concerning the preparation of records for transfer (listing, boxing, notification to Executive Secretariat Records Officer about the records etc.) but to store these archival records in a safe location in your own section/department. Once a Centralized Records building has been constructed, the records can then be transferred immediately. For special situations where records are at high risk of damage or loss and the section/department is not able to provide safe storage for them, please contact the Executive Secretariat Records Officer.

Preparation of Records for Transfer

Identify records to be transferred – Using Nus Records Retention Schedule you will be able to determine which records are permanent and should be transferred to the Main Records Room. Refer to the *Guideline 12 – Sentencing Records* for instructions regarding this process.

Contact the EXECUTIVE SECRETARIAT RECORDS OFFICER – Contact the Executive Secretariat Records Officer for advice and their awareness of the scope of the archival records you are preparing. The Executive Secretariat Records Officer will also provide you with box labels (digital format) and the registration number for this particular transfer. This registration number has to be written on every box (see 'labelling' below).

Use standard archives boxes – Contact the Executive Secretariat Records Officer to advice for the supply of standard archives boxes to be used in the transfer if your records are not already stored in these boxes. They will also provide advice for the packing of oversized items such as large ledgers.

Packing records in boxes – All records have to be clean and free of any insects before being placed into the box. Remove any metal paper clips, bulldog clips and rubber bands. Loose papers must be placed into labelled manila folders (preferably acid free folders) before they are placed into boxes. This includes the contents of arch-lever binders – arch-lever binders are not suitable for archives and therefore should be removed. When placing files in boxes, place them with spines down so they can be easily lifted out. Pack boxes from left to right, with lid attached to your right-hand side. Remember to keep files in their original order as also indicated in the Archives

Transfer List you are providing. Boxes should not be too tightly packed so records can be lifted easily out of the box. Close the box lids but do not tape them.

Labelling the boxes – Each box to be transferred requires a label which is obtained from the Executive Secretariat Records Officer. This label is to be placed on the narrow end of the box with the lid attached to your right-hand side. The labels are used for recording the section/department that transfer the files, transfer registration number and the box number. Label boxes as you go along, and use permanent marker. If you need to do preliminary sorting first, use pencil for any interim marking on the boxes.

Use standard listing template – To make finding records stored in the Archives easier, detailed box lists are very important. Using the standard listing template ensures that all necessary information about the contents is passed on to the Executive Secretariat Records Officer. This template is attached as *Archives Transfer List*. If you have computer resources, it is appreciated if this list is provided in an electronic form in addition to the paper version.

For the transfer to National Archives, also attach the original file index of which the transferred files were a part. Keep a copy of all provided lists in your records.

Listing records – Do not use acronyms unless they are an internationally recognised name e.g. UNESCO, you can also find them in the NUS Classification Scheme. Write years using all four digits e.g. 1968, 2004. Copy exact file numbers and titles as written on covers. If the file title does not explain the contents, add a short description in brackets *e.g. file – 7.1.1 General Staff Manual [2005]*. The date range for a file or bundle of documents, is from the date of the oldest document to the date of the most recent document.

Establish access restrictions – Your section/department may want to restrict public access to certain records even after they are transferred to the Executive Secretariat Records Officer. This must be made following the established procedures. These procedures are explained in *Guideline 2 – Access Restrictions***.** You will need to provide information and VC's authorisation through the '*Access Restriction Form*'. The original of this completed form goes to the Executive Secretariat Records Officer, a copy is filed with your section/department, and another copy is attached on top of each file it refers to.

Transfer Agreements – Your section/department represented by the Manager/director/dean and the Executive Secretariat Records Officer need to sign an agreement for the transfer of the records and their custodianship using the *Transfer Agreement* form. The completed Transfer Lists and any Access Restrictions are to be attached to this agreement.

AUTHORISATION & NOTIFICATION OF RECORDS DESTRUCTION

Document ID *ARD00001*

This form is to be returned to: Executive Secretariat Records Officer
Contact Officer: Cristina Luminita Tuiletufuga **Phone: 20072 ext 113**

Retention Schedule used: "NUS Records Retention Schedule" Approved by VCC Dec 2016

Description of Records Destroyed			
Index No.	**Records electronic Title**	**Date Range**	**Quantity**

I hereby confirm the authorisation of the destruction of the above listed records and that they are destroyed under the provisions of an authorised records retention schedule.

Vice Chancellor of NUS: *Professor Fui Le'apai Tu'ua Ilaoa Asofou So'o*

Date Authorised: ____/____/___ **Signature**_____

Internal Audit of NUS: *Lillian Waterhouse Hytongue*

Date Authorised: ____/____/___ **Signature**_____

Method of Destruction: _____ Date Destroyed: ____/____/___

I confirm that the above listed records are an accurate description of the records destroyed.

Executive Secretariat Records Officer: _____

Date Authorised: ____/____/_____ **Signature**_____

Director Governance Policy and Planning_____

Date Authorised ____/____/_____ **Signature**_____

NUS RECORDS TRANSFER FORM

Document ID *TAG00001*

Section/Department_____ **Box No.**_____

One copy of this form is to be given to ESRO and one to be kept at the section/Department that makes the transfer
Contact ESRO: Cristina Luminita Tuiletufuga **Phone: 20072 ext 113**

Retention Schedule used: "NUS Records Retention Schedule" Approved by VCC Dec 2016

Description of Records Transferred			
Index No.	**Records electronic Title**	**Date Range**	**Other Details**

I hereby accept the transfer of the above listed records and that they will be archived in the Main Records Room of the NUS

DEAN/MANAGER/DIRECTOR *of* **NUS Section/Dpt**_____

Date Authorised: ____/____/___ **Signature**_____

I confirm that the above listed records are an accurate description of the records transferred to the Main Records Room of the NUS.

Executive Secretariat Records Officer _____

Transfer date: ____/____/___ **Signature**_____

NUS RECORDS TRANSFER AGREEMENT

Document ID *TAG00001*

The _____NUS section/department_____**, on this date**_____**,**

hereby confirms their authority to dispose of the records described in the attached transfer list, by transfer them to the Main Records Unit. The _____NUS section/department_____ **and the ESRO agree to transfer the records from the above NUS section/department to the Main Records Room, referring to NUS Records Retention Schedule.**

The _____NUS section/department_____**and the ESRO confirm that the records will be open to the public, with the exception of any records for which access restrictions have been made. The following restrictions are made for records in this transfer:**

□ No access restrictions

□ The attached access restrictions with the access restriction specifications:

_____

_____

_____

_____	_____
(signature)	**(signature)**
_____	_____
(name in print)	**(name in print)**
DEAN/MANAGER/DIRECTOR	**ESRO OF NUS**
NUS Section/Dpt_____	_____
Date signed: _____	**Date signed:** _____