Policy Title	Policy and Procedures for Document Management at UNFPA
Previous title (if any)	
Policy objective	Policy and Procedures for Document Management at UNFPA outlines the mandatory actions, roles and responsibilities for effective document management in UNFPA in order to improve information access, safeguard organizational digital property and preserve institutional memory
Target audience	All UNFPA personnel
Risk control matrix	Controls of the process are detailed in the Risk Control Matrix
Checklist	N/A
Effective date	1 May 2018
Revision History	N/A
Mandatory revision date	May 2021
Policy owner unit	Programme Division
Approval	Policy approved 25 April 2018

Policy and Procedures for Document Management at UNFPA

TABLE OF CONTENTS

I. Purpose

This policy outlines the mandatory actions, roles and responsibilities, and risk mitigation controls for effective document management in UNFPA in order to improve information access, safeguard organizational digital property and preserve institutional memory. Documents are defined as a unit of information that is created, collected or received in the course of UNFPA business, including e-mails, records[1] and other materials in various formats (such as graphics, multimedia and other non-text documents).

II. Policy

This policy outlines UNFPA's document management process, identifies control actions to mitigate potential risks related to the process, and establishes the following:

- All UNFPA documents, regardless of form or medium, are the property of the organization.
- The Integrated Document Management Solution (iDocs) is UNFPA's designated document management platform. All documents shall be managed following the procedures of this policy.
- All UNFPA personnel shall manage their documents through iDocs as specified below:
    - For an internal document[2], the person who shares or finalizes the document is responsible for filing it in the correct iDocs application.
    - For an external document[3], the designated recipient of the document shall be responsible for filing in the correct iDocs application. If there are more than one (1) recipient of a document, the lead on the subject matter of the document shall be the designated recipient.
    - When sharing a document, all personnel shall use the collaborative editing and sharing features of iDocs instead of sending documents as email attachments.
    - When handling sensitive information[4] the responsible personnel must set access control in iDocs following the procedure in this policy to ensure that only authorized personnel determined by the head of office[5] can access it.

[1] Records are defined as "information created, received, and maintained as evidence and information by an organization or person, in pursuance of legal obligations or in the transaction of business."- UN Archives and Records Management Section.

[2] An internal document is a document that is created by a UNFPA personnel.

[3] An external document is a document submitted to UNFPA, such as invoices or reports initiated by a consultant or implementing partner.

[4] Documents created by the UNFPA, received from or sent to third parties that contain information under an expectation of confidentiality.

[5] The UNFPA head of office refers to the representative, division director, regional or sub-regional director, country director or the Chief of Operations (or the delegated officer), as appropriate

- All work-related documents shall be migrated into the [iDocs]-Office-Documents folder before separation from UNFPA, or transfer to a different office or post.

- The head of office shall ensure:
  - Appointment of an iDocs Focal Point for the office;
  - Appointment of an iDocs Library Manager, for all offices that own a corporate library;
  - All personnel in the office manage their documents according to the policy, in order to protect them from loss, damage, unauthorized disclosure or modification;
  - All personnel in the office have successfully completed iDocs e-learning course;
  - All documents with sensitive information are classified, and only personnel authorized by the head of office have access to them;
  - Periodic review of all documents managed by the office, and timely response to requests for document access

- The iDocs Focal Point shall support office members to comply with this policy.

- A Corporate Library Manager shall provide guidance, training and technical support to library users and monitor compliance.

- The iDocs Governance Committee[6] shall provide overall direction for iDocs. The Committee will also review and respond to the requests for the approval of the creation of new corporate libraries.

- A business owner shall obtain endorsement from the iDocs Governance Committee for any new ICT application with a proposed document-upload function prior to submission to the ICT Board.

- This policy comes into effect on 1 May 2018.

III. Procedure

Documents are managed through one of four types of iDocs repositories: i) My Drive, ii) [iDocs]-Office-Documents Management, iii) iDocs Libraries[7] and iv) Records Management.

- All UNFPA personnel shall manage their documents through iDocs as specified in the procedures below.

[6] The iDocs Governance Committee is inter-divisional, and chaired by the Director of Programme Division.

[7] New libraries may be developed upon the approval of the iDocs Governance Committee.

A. **Create a document:** A document can be created in My Drive, [iDocs]-Office-Documents, email, iDocs Library or other applications.

B. **Collaboratively draft a document:** All UNFPA personnel shall use the collaborative features of iDocs for work on a shared document, instead of sending a document as an email attachment. The collaborative features of iDocs allow the document owners to grant, change or revoke rights to edit, comment or view documents at a folder, sub-folder or document level. A document, before sharing for collaborative drafting, must be saved into the [iDocs]-Office-Documents folder.

C. **File a document**: A document can be filed into one of the iDocs repositories as specified in Table 1. All work-related personal documents shall be filed in My Drive. To ensure that all documents only one digital copy in iDocs all personnel shall follow this policy to file internal and external documents. Specific documents that are received in hard-copy form may be scanned and uploaded in the correct iDocs application.

D. **Share a final document:** A final document can be shared with internal and external users for view only for a limited or unlimited time using the document sharing features. Links to a document can also be embedded into emails, websites or other communication documents or sites, subject to the limitations set forth in the Policy of Information Disclosure Policy (2009) and Publications Policy (2013).

E. **Delete a document:** A duplicated document may be deleted from iDocs. If the user accidentally deletes a document in My Drive, the user can recover it from the trash folder. If a user has accidentally deleted a document in the iDocs Library, the library admin will provide support to recover. If a user accidentally deletes a document in [iDocs]-Office-Documents Folder they can contact iDocs Support team through the Integrated Service Desk to recover it.

F. **Migrate documents:** Before separation from UNFPA or transfer to a different office or post, all UNFPA personnel shall migrate all work-related documents into the [iDocs]-Office-Documents folder using the folder upload function, so that any links to the migrated documents will remain valid. The head of office, with support from office iDocs Focal Point(s), shall monitor the process and sign off on document transfer completion status.

Table 1: The types of iDocs repositories

Type	Key Features
My Drive	**Creating, uploading and managing documents in My Drive folder** Each individual personnel with a valid UNFPA email account: • Is assigned a My Drive folder, and is responsible for managing all content in it. • Initiates a draft for sharing or uploads work-related personal documents in My Drive. All documents, once ready to be shared, must be filed in the [iDocs]-Office -Documents folder or iDocs Library when required. • Will change sharing permissions of My Drive folders; including the ability to grant, change or revoke rights to edit, comment, view documents at a folder, sub-folder and document level, as well as to protect sensitive information.
[iDocs]-Office Documents Folder	**Creating, uploading and managing documents in the [iDocs]-Office-Documents folder** The [iDocs]-Office-Documents folder is owned by the office. All personnel in the office can: • Create folders and sub-folders. However, it is highly recommended that the office folder structure and permission settings be managed by the designated office iDocs Focal Point. • Draft and upload documents and manage document sharing, to include granting, changing or revoking rights to edit, comment or view documents at a folder, sub-folder and document level, and to protect sensitive information. • Access to legacy documents that have been migrated from other systems and sources.
Corporate Library	**Development and management of a Corporate Library** • An iDocs library is a UNFPA document repository, normally with automated business process at the corporate level. • To apply for a new library, the head of an office shall request approval by the iDocs Governance Committee to create a corporate library. • The iDocs library is open to authorized personnel with pre-defined access. • The iDocs Library Manager provides technical support and oversees compliance.

Records Management	• Record management component and procedures will be included during the next revision.

- **Handling sensitive information.** To ensure documents that contain sensitive information are protected:
    - Head of office approves information classifications (confidential or strictly confidential). All outgoing and incoming classified information must be recorded in a special registry that lists the staff members who are authorized to handle such information.
    - The creator or recipient of the information concerned, under the overall supervision and guidance of the head of office, shall decide whether the information is confidential, and set access to authorized personnel only at document, sub-folder level and/or folder levels.
    - The head of office shall periodically review and officially classify and declassify the level of confidential information.

  Sensitive information may be classified as "confidential" or "strictly confidential".
    - The designation "confidential" shall apply to information or material whose unauthorized disclosure could reasonably be expected to cause damage to the work of UNFPA, or harm UNFPA, Member States, or individuals.
    - The designation "strictly confidential" shall apply to information or material whose unauthorized disclosure could reasonably be expected to cause exceptionally grave damage to or impede the conduct of UNFPA's work. Inappropriate disclosure of strictly confidential information, for example, might endanger the safety or security of an individual, violate individual rights, invade individual privacy, or endanger the security of Member States.

- **To request a new corporate library,** the head of office shall submit an application through the iDocs Portal.

IV. Other

Not applicable

V. Process Overview Flowchart(s)

Not applicable

VI. Risk Control Matrix

The risk control matrix can be found in the following link:

https://docs.google.com/a/unfpa.org/spreadsheets/d/14xamrGqT_RVvuuYz5M-Pw7b9aJBJs1YDYJaF0enmHeo/edit?usp=sharing