onEvidence Ltd. Cotton Court, Preston PR1 3BY Company #12668322

Document Management Policy

(IGP-3)

Summary			
This Policy establishes standards for document management across all of the Business' functions and operations, and for ensuring documents are created, maintained and disposed of appropriately.			
Scope			
The Policy applies to all staff employed by onEvidence (the Business), including contractors who are carrying out work on behalf of the business.			
Document control			
Document type	Information Governance Policy – IGP-3		
Document owner	Board of Directors		
Lead contact	Dr Roxanne Khan		
Document status	Approved		
Version	V.1		
Approved by	Board	Date	14 April 2023
Date of publication	April 2023	Next review date	April 2025
Date of original publication	April 2023	Review frequency	2 years
Superseded documents	N/A		
Related documents	See 'Interaction with other policies and procedures' below		

Contents

1. **Introduction** 02
2. **Definitions** 02
3. **Purpose of this Policy** 03
4. **Scope of this Policy** 03
5. **Roles and responsibilities** 04
6. **Document management practices** 04
7. **Naming conventions and folder structures** 05
8. **Digital preservation** 05
9. **Destruction** 05
10. **Training** 05
11. **Interaction with other policies and procedures** 05
12. **Policy review and ownership** 06

1. Introduction

Documents are a key part in the effective functioning of any organisation. We need documents on a short-term basis to help us to work consistently and productively and to keep track of progress in projects and activities. Creating standards for document management and ensuring that documents are created, managed and disposed of appropriately is a vital part of good information management that will improve efficiency and mitigate legal and compliance risks. This must also be supported with the necessary guidance and training for staff to ensure they are confident document handlers.

2. Definitions

ISO9000 defines a document as “information and its supporting medium”, meaning that it can include a wide range of both digital and hard copy formats and is not simply limited to written information. It can also be a photograph, video or audio record of an event.

3. Purpose of this Policy

The Business must ensure that documents created in relation to its operations are being managed and maintained appropriately. This Policy sets out standards and definitions to enable staff to create documents that:

- Meet the Business' internal requirements
- Enable the content of the document to be accessed, used and reused in a controlled and efficient manner
- Ensure the continuity of Business operations in the event of staff absence or emergency circumstances
- Are compliant with all regulatory and statutory requirements
- Enable the defence of the rights and interests of the Business and its stakeholders
- Are capable of providing evidence of a decision or operational process
- Are kept and maintained and stored in the most economical way consistent with the above objectives

4. Scope of this Policy

This Policy applies to all staff of the Business and any individual creating or handling documents on the Business' behalf.

The Policy applies to all documents held in any format, including (but not limited to):

- Emails
- Letters (digital and hard copy)
- Policies and guidance
- Meeting papers and minutes
- Reports
- Contracts
- Presentations
- Official communications
- Photographs
- Audio recordings (other than voicemail messages)

Voicemail, text or instant messages do not constitute documents for the purposes of this Policy, unless recorded or retained for specified purposes in accordance with legal requirements. Specific guidance in relation to the processing and storage of research data can be provided by the Board of Directors.

5. Roles and responsibilities

The **Board of Directors** has ultimate responsibility for directing the affairs of the Business and, as such, has operational responsibility for this Policy and ensuring that it complies with legal and regulatory requirements. They are also responsible for monitoring its overall effectiveness.

All staff and third-party contractors are responsible for creating and using documents in line with the terms of this Policy.

6. Document management practices

The below list sets out practices that must be adhered to when creating and handling documents on behalf of the Business:

- Documents must be clearly named (with date and version number if relevant) and stored in a structured manner (see section 8)
- Duplicate copies of documents must not be created unnecessarily
- Wherever possible, documents must be shared from their source location rather than attaching documents to emails
- Key documents (that others may require access to) must be stored in an appropriate shared file store
- Copies of documents, whether digital or hard copy, must only be taken offsite when necessary (encrypted and password-protected removable storage or remote access via a secure network connection must be used whenever possible)
- Digital copies of document should never be emailed to a personal email account or stored on a personal cloud-based storage account
- Once a document is finalised, previous versions and drafts of documents should only be retained where entirely necessary e.g. for audit or legal purposes
- Appropriate metadata (such as title and tags) should be included at the point a new document is created to ensure it can be easily located and retrieved
- Any metadata contained in documents that have been created from previous versions or from templates created by another person should be deleted and/or updated
- Final copies of formal documents (such as policies or minutes) must be saved in PDF format
- Formal documents that will be used and edited in the long term must include a document history or version control box to allow users to see the development of the document over time
- Regular audits (at least annual) of digital and hard copy information must be conducted to ensure that information is not retained longer than it is required

7. Naming conventions and folder structures

A naming convention is a collection of consistent rules followed in naming documents, which should allow users to work effectively, ensure that files can be easily accessed by all who require access and to ensure that individuals are referring to and working on the correct document. The use of consistent naming conventions will improve efficiency by allowing staff to quickly identify the nature of the information contained within a document when searching through an archive or file store. Folder structures and names are also important in allowing the efficient retrieval of documents. The below principles must be followed when creating new folder structures:

- Folders must be clearly named by a relevant subject area
- The names of individuals should only be used when creating a case file
- Top level folders must be kept to a minimum
- Ideally, file structures should not exceed six levels of subfolders
- Appropriate access levels must be assigned depending on necessity to access the documents contained within the folder

8. Digital preservation

Where documents or records are either digitised hard copies or where “born digital”, the Business will ensure that there are appropriate standards and guidance in place to ensure that records of permanent or continuing value remain accessible and preserve their integrity for as long as required, accounting for changes in IT software and hardware.

9. Destruction

The Board of Directors should periodically determine whether any documents under their control have significant operational, informational or evidential value requiring a long-term retention. Documents that do not meet this criterion should be destroyed as soon as they have served their immediate purpose. Such material should not be kept within files, and where it is, the files should be regularly weeded of it.

10. Training

Relevant training and education materials will be provided to ensure that staff are aware of their responsibilities in relation to document management.

11. Interaction with other policies and procedures

The Business has a number of existing policies and procedures that have relevance to information governance, as below, and staff must be aware of their content:

Information Governance Policies:

- Information Governance Policy
- Data Protection Policy
- Information Security Policy

12. Policy review and ownership

This Policy will be reviewed as required and at least every three years by the Board of Directors. The document is managed by Dr Roxanne Khan.