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

Information Governance Policy

(IGP-1)

Summary			
This Policy establishes the key principles of Information Governance at onEvidence and sets out responsibilities and reporting lines for members of staff and provides an over-arching framework for Information Governance across the business.			
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-1		
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Superseded documents	N/A		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** 03
6. **Legal and compliance** 04
7. **Records and document management** 04
8. **Interaction with other policies and procedures** 05
9. **Policy review and ownership** 05

Appendix 1: 06

1. Introduction

Information governance is a decision-making and accountability framework put in place to ensure that the creation, storage, use, disclosure, archiving and destruction of information is handled in accordance with legal requirements and to maximise operational efficiency. It includes the processes, roles, standards and policies that ensure the compliant and effective use of information in enabling an organisation to achieve its goals. Information is a key asset for the Business, and it is vital that measures are in place to manage and control regulatory, reputational and operational risks of poor information governance.

2. Definitions

Information is generally defined as “knowledge or facts about someone or something” and “the communication or reception of knowledge or intelligence”. It can exist in many different formats, but it must have meaning in some context for its receiver. It includes paper-based documents, electronic documents, images, video footage, social media content, statistical or research data, and meta data (being data that are derived from or associated with other data and which describe the characteristics of such data).

Further relevant definitions can be found in Appendix 1.

3. Purpose of this Policy

This Policy is intended to set out the high-level principles of information governance across the Business and to make clear the responsibilities and reporting lines for members of staff. It is intended as an over-arching framework to give clarity about the scope of information governance across the Business and to highlight key information and related policies to staff.

4. Scope of this Policy

This Policy applies to all information held for the purposes of the Business' operations including, but not limited to, the provision of research, psychological services, training, consultancy, staff support, internal and external reporting and publications. It applies to information created by staff members of the Business and also to information received from third parties.

This Policy applies to all staff employed by the Business, including contractors who are carrying out work on behalf of the business.

5. Roles and responsibilities

Board of Directors

The Board of Directors has ultimate responsibility for directing the affairs of the Business and, as such, will ensure the Business has appropriate information governance procedures in place to mitigate risk and maximise the value of the information it holds.

All staff and third-party contractors

All members of Business staff, including contractors who are carrying out work on behalf of the business, are responsible for ensuring that they are aware of the requirements of the Business' policies in relation to information governance and security and adhere to them on a day to day basis. All staff are responsible for highlighting areas of perceived risk where information practices could be improved and to report any incidents that could be considered a breach of the Business' internal policies or external legislation.

All staff will be required to enter into confidentiality obligations with the Business and to participate in information governance training during induction and periodically throughout their employment or engagement. Any breach of confidentiality and/or the Business' information governance and security policies may be a contractual and/or disciplinary matter which could result in termination of an individual's employment or engagement by the Business.

6. Legal and compliance

The Business' information governance framework must ensure compliance with various pieces of legislation relating to the handling and use of information, as well as the common law duty of confidentiality. These include, but are not limited to:

- Data Protection Act 2018
- General Data Protection Regulation (Regulation (EU) 2016/679)
- Freedom of Information Act 2000
- Privacy and Electronic Communications (EC Directive) Regulations 2003 (as amended)
- Environmental Information Regulations 2004
- Regulation of Investigatory Powers Act 2000
- Computer Misuse Act 1990
- The Telecommunications (Lawful Business Practice) Regulations 2000
- Human Rights Act 1998
- Copyright, Designs and Patents Act 1988
- Official Secrets Act 1989
- Malicious Communications Act 1988
- Digital Economy Act 2010
- Intellectual Property Act 2014
- Investigatory Powers Act 2016

There also other non-legislative compliance requirements the Business must adhere to (both internal and external), such as:

- Requirements set out by ethics committees and in line with other regulatory or institutional approvals
- Requirements detailed in funding and contract terms

7. Records and document management

The Business' Document Management Policy sets out the consistent standards that staff should use when creating, using and disposing of information.

Training

The Business will ensure relevant training is in place to assist staff in their day to day handling of information.

8. 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:

- Data Protection Policy
- Document Management Policy
- Information Security Policy

9. 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.

Appendix 1: Definitions

Information

Information is generally defined as “knowledge or facts about someone or something” and “the communication or reception of knowledge or intelligence”. It can exist in many different formats, but it must have meaning in some context for its receiver.

Documents

ISO9000 defines a document as “information and its supporting medium”, so it can include a wide range of both hard copy and digital formats and is not simply limited to written information. Documents can be created in many formats, including (but not limited to):

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

Records

ISO defines records as: “...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.” Records are a subset of information and documents.

Document management

The field of management that is responsible for the efficient and systematic control of the creation, distribution, use, maintenance and disposal of documents.