Information Management

Policy

Information Management Policy

1. Introduction

Information is one of our key assets which should be governed and managed effectively. The information we use, in the form of emails, databases, electronic or paper records, represents our “corporate memory” and is a vital asset for our ongoing operations providing valuable evidence of business activities and transactions as well as protecting our corporate assets.

At Keller we are committed to both making information more easily accessible to those who need it and to keeping our employee and customer records and identifying information confidential to the extent that the law permits.
The successful implementation of an information management policy will help to achieve this, as well as to maintain high standards of customer service, operate our business efficiently, meet legal and regulatory requirements across all jurisdictions in which we operate and protect our corporate assets.

This policy adheres to the Data Protection Act 2018 and all equivalent legislation in other jurisdictions in which Keller operates or has a presence.

2. Policy objectives

We are committed to:

- Maintaining a governance framework to support business processes to improve and sustain information quality;
- Ensuring we understand business needs for the key information we create, acquire, use, store and report;
- Developing and maintaining clear policies and procedures for all key pieces of information to ensure we manage information effectively to meet business needs (both electronically and in hard copy form);
- Implementing appropriate means of security for our information and corporate assets;
- Introducing mechanisms to help us comply with these policies and procedures; and
- Providing guidance, training and support to staff where required.

The benefits of properly managing information can be significant and more than financial in nature. It helps to improve trust ,efficiency ,security, and by meeting regulatory and legislative requirements we reduce the risk of financial penalties and reputational damage. This policy covers four key areas:

1. ***Information Privacy***
   Keller will seek to ensure personal data is adequately protected.
2. ***Information Retention & Disposition***
   Keller will require that necessary records and documents are adequately protected and maintained whilst ensuring that records no longer needed, or deemed to have no further value, are discarded at the appropriate time according to their disposal schedules.
3. ***Information Quality***
   Keller shall require that high standards of information quality will be maintained at all times.
4. ***Information Classification***
   To satisfy legal and regulatory requirements, Keller will classify and categorize corporate information assets using a risk-based approach. By doing so, Keller will convey the required safeguards for information confidentiality, integrity and availability.

3. Delivering our objectives

Keller will make arrangements to promote this Policy to ensure that:

- All information created and acquired meets business needs;
- Information is accessible to whoever needs it and is fit for the purpose required;
- Information retained is relevant to business objectives and only kept for the period required;
- Information is properly classified to identify where to apply standards and prioritise focus;
- Information is secured in accordance with the security classification defined;
- Any piece of information held, captured or created by our record keeping systems will represent the corporate master record source and will not be duplicated unnecessarily;
- We understand the requirements to maintain the quality of information and regularly measure and report compliance; and
- Information is properly and securely disposed of when it is no longer required.

4. Scope

This policy applies to all legal entities which Keller Group plc wholly owns, has a majority stake in or overall operational control of.

The Information Management policy is concerned with all information, which means information that is created, acquired, used, stored, reported or disposed of in the course of business, or its employee, customer and other stakeholder information.

5. Governance

The Data Protection Steering Committee provides oversight of this policy.

6. Responsibilities

This policy applies to all individuals who are employed by, or carry out work on behalf of, any Keller group company including contractors, temporary staff and agency workers.

7. Supporting information

- Code of Business Conduct
- Quality & Continuous Improvement Policy
- Information Security Policy
- Data Protection Policy

8. Document change history

Policy status	FINAL
Issue date	17.10.2016
Version last reviewed and updated	July 2022
Policy owner	Group Legal Function