IChemE ADVANCING CHEMICAL ENGINEERING WORLDWIDE

Information governance policy

Document control

Version	Date issued	Changes
V2.0	7 August 2019	Baselined for release
V1.4	5 June 2019	Examples of Information Assets provided
V1.3	24 May 2019	Addressing typos
V1.2	20 May 2019	Addressing comments from Mills & Reeve
V1.1	18 May 2019	Comments from Mills & Reeve
V1.0	2 May 2019	New document

Information governance policy

Introduction

This policy should be read in conjunction with the following documents which can be found at www.icheme.org/policies:

- Data Breach Procedure
- Data Protection Policy
- Data Sharing Policy
- Individual Data Rights Request Procedure
- Information Security Policy
- Records Retention Policy
- Website terms of use and Privacy Policy

Purpose and scope

This policy establishes the key high-level principles of information governance and document management at IChemE and sets out responsibilities and reporting lines for members of staff. It provides an over-arching framework for information governance across the Institution.

The policy applies to all staff, contractors or any other person with access to Information Assets owned by IChemE.

Background

At its simplest information governance is an accountability and decision-making framework. It is put in place to ensure that the creation, storage, use, disclosure, archiving and destruction of information is handled in accordance with good practice, legal requirements and to maximise operational efficiency. It includes the processes, roles, policies and standards that ensure the compliant and effective use of information in enabling an organisation to achieve its goals.

Information is a key asset for IChemE and the regulatory, reputational and operational risks of poor information governance are ever increasing. As the creation of information proliferates, it is vital that IChemE has measures in place to manage and control these risks.

Definitions

Documents

A document is defined 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):

- letters (digital and hard copy)
- emails
- policies and guidance
- meeting papers and minutes
- reports
- contracts
- presentations
- official communications
- photographs
- audio recordings

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.

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.

Information Security

The purpose of information security is to protect and preserve the confidentiality, integrity, and availability of information. It may also involve protecting and preserving the authenticity and reliability of information and ensuring that entities can be held accountable.

Information assests

The National Archives defines an information asset as "a body of information, defined and managed as a single unit so it can be understood, shared, protected and exploited effectively". There are no set rules in defining what an information asset is, but it must be categorised in a way that is understandable and useful to IChemE, its members and its staff. It can be a single document or a group of related documents.

Examples of items that can be information assets include:

- strategies, plans, goals and objectives that have been developed to improve IChemE's future
- information that is sold as a product or a service such as a book/publication or a research tool
- any intellectual property developed and owned by IChemE
- project information such as requirements, delivery plans etc
- training materials and content
- marketing and/or sales collateral
- customer lists ie member data and non-member data
- operations information such as Standard Operating Procedure (SOP)
- decision support tools
- financial information such as financial accounts or reporting data
- organisational culture information such as team charters or principals.

Information Asset Register

The Information Asset Register documents all IChemE's information assets, IAOs and associated relevant information. It is managed and updated by the Information Governance Advisors in the Privacy Team on an annual basis.

Records

Records are defined 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.

Roles and responsibilities

There are a number of key roles and responsibilities across IChemE in relation to information governance, as set out below.

Senior Information Risk Owner (SIRO)

The SIRO is accountable at a senior management level for ensuring that IChemE has robust information governance and security processes and procedures in place. This role is held by the Director of Finance.

Information Asset Owners (IAOs)

IAOs are appropriately senior members of staff who have responsibility for specific information assets. Their role is to ensure those assets are handled and managed properly, that appropriate access and security controls are in place and that the accuracy and integrity of the information is assured. They provide assurance to the SIRO that where an information risk is identified it is being managed effectively. If an IAO identifies an issue in relation to an information asset they must notify the SIRO via the Information Governance Advisors – the Privacy Team.

Information Governance Advisors

Information Governance Advisors will oversee the information governance framework to ensure that it is operating effectively and assist the SIRO and IAOs with advice and guidance in relation to the handling and use of information. This role will also be responsible for managing IChemE's Information Asset Register. In the interim this role will be fulfilled by the Privacy Team.

Legal and Compliance

IChemE's 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
- The Telecommunications (Lawful Business Practice) Regulations 2000
- Human Rights Act 1998
- Copyright, Designs and Patents Act 1988
- Official Secrets Act 1989
- Malicious Communications Act 2010
- Digital Economy Act 2010
- Intellectual Property Act 2014
- Investigatory Powers Act 2016

There are also non-legislative compliance requirements such as:

- Information Security Policy
- Payment Card Industry Data Security Standards
- requirements stipulated by contract.

Document lifecycle

All documents created have a 'lifecycle' from creation through to disposition, as shown below:

It is important to understand this cycle and the various stages when creating and handling documents to ensure that they are managed effectively.

Creation

Documents that will represent formal, compliant, and trusted communications or records must be well-designed from the point of creation, using relevant naming conventions and document templates when necessary.

Distribution

The act of sharing a document with others internally or externally.

Use

Use takes place after a document has been distributed, and can generate business decisions, further actions, or serve other purposes.

Maintenance

While a document is in active use, it is vital that the content is maintained, accurate and available to those who require it at all times.

Disposition

The practice of handling information that is accessed less frequently or has reached its assigned retention period. The Records Retention Policy sets out retention periods for various categories of information.

Document management practices

The list below sets out practices that must be adhered to when creating and handling documents on behalf of IChemE. As SharePoint is rolled out it is expected that this list will grow.

- once SharePoint has been rolled out to all departments all documents will be created in SharePoint unless there are exceptional reasons to the contrary. In the interim period prior to SharePoint being rolled out documents will continue to be created and managed via the relevant legacy system;
- documents must be clearly named (with date and version number if relevant) and stored in a structured manner – 20190520 v0.1 draft Information Security Policy;
- duplicate copies of documents must not be created unnecessarily;
- any sharing of documents should where possible take place via the use of SharePoint and/or Onedrive sharing capabilities;
- the use of email and/or third party systems should be limited to where strictly necessary and where the risks of using these channels of communication are understood and recognised on the Information Risk Register;

- digital copies of documents should never be emailed to a personal email account or stored on a personal cloud-based storage account. Hard copies should only be retained where necessary and stored on IChemE premises;
- once a document is finalised, previous versions and drafts of documents should only be retained where entirely necessary eg for legal or audit 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.

Led by members, supporting members and serving society

Contact us for further information

UK
t: +44 (0)1788 578214
e: membersupport@icheme.org

Australia
t: +61 (0)3 9642 4494
e: austmembers@icheme.org

Malaysia
t: +603 2283 1381
e: malaysianmembers@icheme.org

New Zealand
t: +64 (0)4 473 4398
e: nzmembers@icheme.org

Singapore
e: singaporemembers@icheme.org

LC 0050_20