IChemE ADVANCING CHEMICAL ENGINEERING WORLDWIDE

Information security policy

Document control

Version	Date issued	Changes
V2.0	7 August 2019	Baselined for release
V1.9	5 July 2019	Amendment to the Encryption
V1.8	13 June 2019	Amendment to differentiate between Restricted and Confidential
V1.7	30 May 2019	Amendments to cover withdrawal of access
V1.6	20 May 2019	Baselined version
V1.5	20 May 2019	Addressing comments from Mills and Reeve
V1.4	18 May 2019	Further comments from Mills and Reeve
V1.3	2 May 2019	Addressing comments from Mills and Reeve
V1.2	1 May 2019	Comments from Mills and Reeve
V1.1	17 April 2019	Draft comments from IT
V1.0	19 March 2019	New document

Content

Document control

Information security 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 Governance Policy
- Records Retention Policy
- Website terms of use and Privacy Policy

Purpose and scope

This policy is concerned with the management and security of IChemE's information assets and the use made of these assets by its employees, members, suppliers and others who may legitimately process information on behalf of IChemE.

An effective Information Security Policy provides a sound basis for defining and regulating the management of information systems and other information assets. This is necessary to ensure that information is appropriately secured against breaches of confidentiality, integrity, availability.

The policy applies to all information assets which are owned by IChemE, used by IChemE for business purposes or which are connected to any networks managed by IChemE.

Definitions of reoccurring terms used throughout this policy are provided at Appendix A.

Principals

The following principles underpin the policy:

1. Information should be classified according to an appropriate level of confidentiality, integrity and availability (see Information Classification) and in accordance with relevant legislative, regulatory and contractual requirements.
2. Information must be handled in accordance with its classification level.
3. All users covered by the scope of this policy must handle Information Assets appropriately and in accordance with its classification level.
4. Information should be both secure and available to those with a legitimate need for access in accordance with its classification level.
5. Information will be protected against unauthorised access and processing in accordance with its classification level.
6. Breaches of this policy must be reported (see Compliance and Incident Handling).
7. Information security provision and the policies that guide it will be regularly reviewed, including through the use of annual internal audits and penetration testing.

Information classification

The following table provides a summary of the information classification levels that have been adopted by IChemE and which underpin the principles of information security defined in this policy. These classification levels explicitly incorporate the General Data Protection Regulation's definitions of criminal offence data, personal data and special categories of personal data, as laid out in IChemE's Data Protection Policy.

Security level	Description	Examples
Restricted	Highly sensitive information that would potentially cause harm if not protected. 'Restricted' identifies that the information is limited to named individuals eg CEO, Financial Director, Payroll Administrator.	Special Category data and Criminal Offence data as defined under GDPR. Financial data. Passwords. Some business sensitive draft reports, papers and minutes. Draft and Full reports that includes personal data eg grievance reports.
Confidential	Highly sensitive information that would potentially cause harm if not protected. 'Confidential' identifies that the information is limited to a group of people eg budget holders.	Special Category data and Criminal Offence data as defined under GDPR. Financial data. Passwords. Some business sensitive draft reports, papers and minutes. Draft and Full reports that includes personal data eg grievance reports.
Internal use	Information that has not been designed for public consumption.	Draft reports, papers and minutes. Employee handbooks and policies.
Public	Information that can be shared with the public.	Press releases. Statutory Accounts.

An Information Asset Register will be collated and maintained by the Privacy Team that lists all IChemE Information Assets, the Asset owner and the date the Asset was last reviewed. The register will be based on information gathered during periodic reviews. Outside of these reviews reasonable steps will be taken to keep it appropriately updated.

User management and eligibility

Access to IChemE information systems must be restricted to authorised users. Accounts will only be issued to those who are eligible for an account and whose identity has been verified. User accounts will only be provided for:

- employees
- backup technology
- 848, and
- Business Cloud Integration.

Authorisation to manage

The management of user accounts and privileges on IChemE's information systems is restricted to suitably trained and authorised members of staff within IT.

Account and privilege management

When an account is created, a unique identifier (userID) will be assigned to the individual user for their individual use. This userID may not be assigned to any other person at any time (userID's will not be recycled). On issue of account credentials, users must be informed of the requirement to comply with this policy.

Access rights granted to users will be restricted to the minimum required in order for them to fulfil their roles.

Procedures shall be established for all information systems to ensure that users' access rights are adjusted appropriately and in a timely manner to reflect any changes in a user's circumstances (eg when a member of staff changes their role or a member of staff leaves IChemE).

Privileged accounts are accounts used for the administration of information systems and are distinct from user accounts. These accounts must only be used by system administrators when undertaking specific tasks which require special privileges. System administrators must use their user account at all other times.

Encryption

All PCs and Laptops are protected via a bios level system password. This prevents unauthorised access by not allowing a user to get as far as the windows login screen unless they enter the correct password.

As part of the Windows 10 standard image build and deployment, all Windows laptops will have BitLocker encryption provisioned. BitLocker is a full volume encryption feature which protects the information on the whole disk by converting it into unreadable code that cannot be deciphered easily by unauthorised people. Thus mitigating the risk from lost or stolen laptops.

Data sharing encryption

IChemE's chosen method for sharing data is via SharePoint\OneDrive links. Data is not to be sent via email.

Where it is not possible to use this method due to security restrictions being in place.

Data should be encrypted using MS Word or Excel inherent password & encryption protection before it is sent. Please bear in mind IT does not have the tools to reset forgotten passwords.

Password management

As part of the account provisioning process, the user may need to be informed of an initial, temporary password. This password must be communicated to the user in a secure way and must be changed by the user immediately.

Users will be prompted on a regular basis to update their passwords.

You must:

- **only log on to IChemE's computer systems using your own password**
- **keep your password secret**
- **select a password with is not easily broken (eg not your surname)**
- **lock your screen if you step away from your device.**

You are not permitted to use another employee's password to log on to the computer system, whether or not you have that employee's permission. If you log on to any IChemE provided device using another employee's password, you may be liable to disciplinary action which could result in dismissal for gross misconduct. If you disclose your password to another employee, you may also be liable to disciplinary action.

Compliance

Any security breach of IChemE's information systems could lead to the possible loss of confidentiality, integrity and availability of personal or other confidential data stored on these information systems. The loss or breach of confidentiality of personal data may be an infringement of the General Data Protection Regulation, contravene IChemE's Data Protection Policy, and may result in regulatory, civil or criminal action against IChemE and/or its employees/agents.

The loss or breach of confidentiality of contractually assured information may also result in the loss of business, financial penalties or criminal or civil action against IChemE. Therefore it is crucial that all users of the organisation's information systems adhere to this policy.

All current staff, members and other authorised users are required to read this policy. Security breaches will be handled in accordance with all relevant policies, including the appropriate disciplinary policies.

Incident handling

If an employee, member or other person with authorised access to IChemE's information systems is aware of an information security incident then they must immediately report it to the Privacy Team and or their line manager.

Examples of information security incidents include but are not limited to:

- unauthorised access to, or use of, IChemE systems, software or data
- unauthorised changes to IChemE systems, software or data
- loss or theft of equipment used to store, or work with, sensitive data
- compromised user accounts.

Monitoring

IChemE may carry out monitoring of employees, workers and contractors. Monitoring may be necessary either to allow IChemE to perform its contract with an employee, worker or contractor, or for IChemE's own legitimate interests.

IChemE's reasons for monitoring include:

- security and the prevention and detection of crime
- ensuring appropriate use of IChemE's telecommunications and computer systems
- ensuring compliance with regulatory requirements
- monitoring attendance, work and behaviour.

The monitoring carried out may include:

- monitoring of premises using video cameras
- monitoring of emails and analysing email traffic
- monitoring websites visited by employees using IChemE systems
- recording telephone calls and checking call logs
- monitoring the use of IChemE vehicles via vehicle-tracking systems
- entry and exit systems, including the use of biometric data such as fingerprints
- tracking via mobile devices.

IChemE may use information gathered through employee monitoring as the basis for disciplinary action against employees. If disciplinary action results from information gathered through monitoring, you will be given the opportunity to see or hear the relevant information in advance of the disciplinary meeting. IChemE will ensure data collected through monitoring is processed in accordance with the IChemE's Data Protection Policy and data protection legislation and, in particular, it will be kept secure and access will be limited to authorised individuals.

IChemE reserves the right to introduce additional monitoring. Before doing so, IChemE will:

- identify the purpose for which the monitoring is to be introduced;
- ensure that the type and extent of monitoring is limited to what is necessary to achieve that purpose;
- where appropriate, consult with affected employees in advance of introducing the monitoring;
- weigh up the benefits that the monitoring is expected to achieve against the impact it may have on employees.

IChemE will ensure employees are aware of when, why and how monitoring is to take place and the standards they are expected to achieve.

If IChemE has reason to believe that certain employees are engaged in criminal activity, IChemE may use covert monitoring to investigate that suspicion. In such instances, any monitoring will take place under the guidance of the police and will be carried out in accordance with data protection legislation.

Examples of misuse include, but are not limited to, the following:

- accessing online chat rooms, blogs, social network sitres - except where explicitly authorised as part of your role;
- use of online auction sites;
- sending, receiving, downloading, displaying or disseminating material that discriminates against, degrades, insults, causes offence to, or harrasses others;
- accessing web pages or files downloaded from the internet that could in any way be regarded as illegal, offensive, or inappropriate in a professioinal environment;
- accessing pornographic or other inappropriate or unlawful materials;
- engaging in online gambling;
- forwarding electronic chain letters or similar materials;
- downloading or disseminating copyright materials;
- issuing false or defamatory statements about any person or organisation via IChemE's electronic systems;
- unauthorised sharing of confidential information about IChemE or any person or organisation connected to IChemE;
- unauthorised disclosure or personal data; and
- loading or running unauthorised games or software.

Any evidence of misuse may result in disciplinary action which may result in summary dismissal. If necessary, information gathered in connection with the investigation may be handed to the police.

Acceptable use

IChemE's computer systems, software and their contents, including IChemE email accounts, belong to IChemE and they are intended for business purposes only.

You are only permitted to use IChemE's computer systems in accordance with IChemE's data protection policy and the following guidelines.

Responsibilities

You are permitted to use IChemE's systems, including internet browsing for personal use on a limited basis and as long as this doesn't interfere with your responsibilities.

You are not permitted to download or install software from external sources (Ie any source outside the IChemE network) unless you have express authorisation from IT. No device or equipment should be attached to IChemE's systems without prior approval from IT.

You should take care when opening emails and/or documents from unknown origins. Attachments may be blocked if they are deemed to be potentially harmful to IChemE's systems.

All information, documents, and data created, saved, or maintained on IChemE's computer system remains at all times the property of IChemE.

Complaints of bullying and harassment

If you feel that you have been harassed or bullied or are offended by material received from a colleague, you should inform your manager immediately. Further information can be found in the Grievance Policy and the Employee Handbook.

Processing personal data

You may have access to the personal data of other individuals and of our customers and clients that is being processed within IChemE's computer systems in the course of your employment. Where this is the case, IChemE relies on you to help meet its data protection obligations to all data subjects including employees, to customers and clients.

If you have access to personal data, you are required:

- to access only data that you have authority to access and only for authorised purposes;
- not to disclose data except to individuals (whether inside or outside IChemE) who have appropriate authorisation;
- to keep data secure by complying with rules on access to premises, access to computers including password protection, and secure file storage and destruction;
- not to remove personal data, or devices containing or that can used to access personal data, from IChemE's premises without adopting appropriate security measures (such as encryption or password protection) to secure the data and the device; and
- not to store personal data on local drives or on personal devices that are used for business purposes. Storage on your IChemE provided OnDrive is permitted with the agreement of your line manager.

Failure to observe these requirements may amount to a disciplinary offence which will be dealt with under IChemE's disciplinary procedure. Significant or deliberate breaches of this policy, such as accessing employee, customer or client data without authorisation or a legitimate reason to do so, may constitute gross misconduct and could lead to your dismissal.

Where IChemE has reason to suspect actions in violation of this policy or is notified by a supplier/partner that it should intervene to mitigate the risk of actions that are in violation of this policy, IChemE has the right to temporarily suspend access to a user account. Where a suspension is actioned this will either be until an investigation is complete or some other identified trigger point. It will be at the discretion of the relevant senior manager authorising a suspension to determine whether the individual should be informed at point of suspension given all the relevant known facts.

Devices

Personal devices

Whilst IChemE does not require employees to use their own personal devices for work purposes, it is recognised that this is often convenient and such use is permitted subject to the following requirements and guidelines.

Users must at all times give due consideration to the risks of using personal devices to access IChemE information and in particular, information classified as confidential or above:

- the device must run a current version of its operating system. A current version is defined to be one for which security updates continue to be produced and made available to the device;
- mobile devices must be encrypted. (Some older devices are not capable of encryption and these should be replaced at the earliest opportunity);
- an appropriate passcode/password must be set for all accounts which give access to the device;
- a password protected screen saver/screen lock must be configured;
- the device must be configured to 'autolock' after a period of inactivity (no more than 10 minutes);
- devices must remain up to date with security patches both for the device's operating system and its applications;
- devices which are at risk of malware infection must run anti-virus software;
- all devices must be disposed of securely;
- the loss or theft of a device which has been used for business reasons must be reported to IT Services;
- any use of personal devices by others (family or friends) must be controlled in such a way as to ensure that these others do not have access to unrestricted IChemE information assets;
- do not send or receive business related documents on your personal phone or laptop;
- if discussing business matters over any form of instant messaging platform on your device, employees should refrain from using names of any customer, member, or professional connection.

In addition to the above requirements, the following recommendations will help further reduce risk:

- consider configuring the device to 'auto-wipe' to protect against brute force password attacks where this facility is available;
- consider implementing remote lock/erase/locate features where these facilities are available;
- do not undermine the security of the device (eg by 'jail-breaking' or 'rooting' a smartphone);
- do not leave mobile devices unattended where there is a significant risk of theft;
- be aware of your surroundings and protect yourself against 'shoulder surfing';
- minimise the amount of restricted data stored on the device and avoid storing any data classified as confidential;
- access restricted information assets via IChemE's remote access facilities wherever possible rather than directly;
- be mindful of the risks of using open (unsecured) wireless networks. Consider configuring your device not to connect automatically to unknown networks;
- if a personally owned device needs to be repaired, ensure that the company you use is subject to a contractual agreement which guarantees the secure handling of any data stored on the device;
- reduce the risk of inadvertently breaching data protection legislation by ensuring that all data subject to the Act which is stored on the device is removed before taking the device to a country outside of the European Economic Area (or the few other countries deemed to have adequate levels of protection).

IChemE owned devices

IChemE may at times provide computing devices such as smartphones or tablets. When it does, it will supply devices which are appropriately configured so as to ensure that they are as effectively managed as other devices such as desktop PCs or laptops. Devices supplied by IChemE must meet the minimum security requirements listed on the previous page for personally owned devices.

Any IChemE owned device may be used for limited personal use (see Acceptable Use).

Where an IChemE owned device is provided:

- family and friends must not make any use of the supplied devices
- no unauthorised changes may be made to the supplied devices, and
- all devices supplied must be returned to IChemE when they are no longer required, in the event of termination of employment, or at the request of IChemE.

Appendix A - Definitions

Encryption

The process for securing data and restricting use to authorised personnel

GDPR

The General Data Protection Regulation, which came into force in May 2018. It should be read alongside the Data Protection Act 2018, which covers the limited areas where the UK can outline how the Regulations take affect in this country.

Information Assets

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 the University and its staff. It can be a single document or a group of related documents.

Information Systems/Information Storage Systems

A network, drive, database owned by IChemE or a third party where IChemE has a contractual relationship that facilitates the systematic storage of Information Assets. Examples include but are not limited to:

- CRM - NG or Dynamic 365
- SharePoint and OneDrive
- S Drive
- Umbraco Content Management System
- Access Dimensions
- EventsForce
- Shopify.

Personal Data

GDPR defines personal data as any information relating to an identified or identifiable natural person ('data subject'). An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Special Category Data

GDPR defines special category data as personal data which satisfies any of the following conditions:

- personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs
- trade-union membership
- genetic data, biometric data processed solely to identify a human being
- health-related data
- data concerning a person's sex life or sexual orientation.

These definitions are broadly analogous to the concept of sensitive data set out in the Data Protection Act 1998.

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