Scope: Although chapters of ISM are separate legal entities and are independently required to comply with all laws and regulations, ISM is providing this template policy to promote compliance, consistency and standards, required to be associated with the ISM brand and license agreement.

**Data protection policy**

ISM—[Chapter name], Inc. needs to gather and use certain information about individuals.

These can include customers, suppliers, business contacts, employees and other people the chapter has a relationship with or may need to contact. This policy describes how this personal data must be collected, handled and stored to meet data protection standards — and to comply with the law.

**Why this policy exists**

This data protection policy ensures ISM—[ Chapter name], Inc.:

* Complies with data protection law and follows good practice
* Protects the rights of staff, customers and partners
* Is transparent about how it stores and processes individuals’ data
* Protects itself from the risks of a data breach

**Data protection law**

The Data Protection Act 1998 describes how organizations — including ISM—[ Chapter name], Inc. — must collect, handle and store personal information.

These rules apply regardless of whether data is stored electronically, on paper or on other materials.

To comply with the law, personal information must be collected and used fairly, stored safely and not disclosed unlawfully.

This policy applies to chapter officers, chapters, staff, contractors, suppliers and others working on behalf of ISM—[Chapter name], Inc.

This policy applies to all data that the chapter holds relating to identifiable individuals, even if that information technically falls outside of the Data Protection Act 1998. This can include individual names, mailing address, email address, phone numbers and any other information relating to individuals.

**Data protection risks**

This policy helps to protect ISM—[Chapter name], Inc. from data security risks, including:

* **Breaches of confidentiality.**
* **Failing to offer choice** to individuals about how their personal data is used.
* **Reputational damage.**

**General guidelines**

* The only people able to access data covered by this policy should be those who **need it for their work**.
* Data **should not be shared informally**.
* Chapter officers/volunteers should keep all data secure, by taking sensible precautions and following the guidelines below.
* In particular, **strong passwords must be used** and they should never be shared.
* Personal data **should not be disclosed** to unauthorized people, either within the chapter or externally.
* Data should be **regularly reviewed and updated** if it is found to be out of date. If no longer required, it should be deleted and disposed of safely.
* Chapter officers/volunteers **should request help** from the chapter president or ISM Global, if they are unsure about any aspect of data protection.

**Data storage**

These rules describe how and where data should be safely stored. Questions about storing data safely can be directed to the chapter president or executive officer/secretary.

When data is **stored on paper,** it should be kept in a secure place where unauthorized people cannot see it.

These guidelines also apply to data that is usually stored electronically but has been printed out.

* When not required, the files should be kept **in a locked drawer or filing cabinet**.
* **Data printouts should be shredded** and disposed of securely when no longer required.

When data is **stored electronically**, it must be protected from unauthorized access, accidental deletion and malicious hacking attempts:

* Data should be **protected by strong passwords** that are changed regularly and never shared between officers/volunteers.
* If data is **stored on removable media**, these should be kept locked away securely when not being used.
* Data should only be stored on **designated drives and servers**, and should only be uploaded to an **approved cloud computing services**. (i.e., ISM portal, Star Chapter, etc.)
* Servers containing personal data should be **sited in a secure location**.
* Data should **never be saved directly** to laptops or other mobile devices like tablets or smart phones.

**Subject access requests**

All individuals who are the subject of personal data held by ISM—[ Chapter name], Inc. are entitled to:

* Ask **what information** the company holds about them and why.
* Ask **how to gain access** to it.
* Be informed **how to keep it up to date.**
* Be informed how the company is **meeting its data protection obligations**.

If an individual contacts the chapter requesting this information, this is called a subject access request. Subject access requests from individuals should be made by email, addressed to the [select chapter position] at [email address].

Individuals, may be charged a nominal fee up to $10 per subject access request. The chapter should provide the relevant data within 14 days. The chapter will always verify the identity of anyone making a subject access request before handing over any information.

The chapter must have procedures on data storage and subject access verification.

**Disclosing data for other reasons**

In certain circumstances, the Data Protection Act allows personal data to be disclosed to law enforcement agencies without the consent of the data subject.

Under these circumstances, ISM—[Chapter name], Inc. will disclose requested data. However, the chapter will ensure the request is legitimate, seeking assistance from the board and from the legal advisors as necessary.