IHSGB Ltd : Records Management Policy (Policy Statement Regarding: Data Protection, Secure Storage, Handling, Use, Retention and Disposal of Disclosure Information)

IHSGB LTD. complies fully with its obligations under the Data Protection Act 1998 and is working towards full compliance with the new GDPR due to be implemented 25th May 2018.

1. Introduction

IHSGB LTD. recognises that its records are an important asset and are a key resource to effective operation and to accountability. The Society also has responsibility for holding member's information and each Officer of the Society has responsibility for any records they hold.

Like any asset, records require careful management and this policy sets out the Society's responsibilities and activities in regard to the management of its records.

2. Principles underpinning the Policy

a. The Records Management Policy applies equally to paper and electronic records.
b. Data Protection Principle 5 (DP5) applies to all records. This states that: "Personal Data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes".
c. The Lord Chancellor's Code of Practice (2009) under FOIA applies to all records. This states at 12.2: 'Records should only be retained for as long as they are needed by the organisation, for reference or accountability purposes, to comply with regulatory requirements or to protect legal and other rights and interests'.
d. No record is to be maintained unless there is a legitimate and identifiable reason for doing so.

3. Scope

This policy aims to ensure that records are managed effectively throughout the organisation, in accordance with professional principles and specified legislation and guidelines. It applies to all the records of the Society. A record is any recorded information regardless of medium (including paper, electronic, audio-visual and record copies of publications), which is created, collected, processed, used, stored and/or disposed of by, employees, as well as those acting as its agents in the course of a Society activity. It applies to all Officers of the Society.

4. Policy Statement

The aim of the policy is to define a framework for managing the Society's records to ensure that the Society:

a. Creates and captures authentic and reliable records to demonstrate evidence, accountability and information about its decisions and activities
b. Facilitates auditing and protects our legal and other rights
c. Maintains records securely and preserves access to them
d. Disposes appropriately of records that are no longer required
e. Protects vital records, which it needs to order to function effectively
f. Maintains records to meet the Society's business needs
g. Addresses the needs of the Society's stakeholders
h. Conforms to any legal and statutory requirements relating to recordkeeping
i. Complies with government directives.

6 Training and Awareness

Since all Trustees and Officers are involved in creating, maintaining and using records, it is vital that everyone understands their record management responsibilities as set out in this policy.

Training can be arranged for Society Officers to ensure that all are aware of their obligations around Data Protection, Freedom of Information and Records Management.

7. Records Creation, Keeping & Maintenance

Record keeping will

a. Document all activities.
b. Provide for quick and easy retrieval of information.
c. Take into account the legal and regulatory environment specific to the area of work.
d. Link records with any Freedom of Information Scheme.
e. Reference, title, index and version control and security mark records as applicable.
f. Keep the system updated.
g. Provide the ability to cross reference electronic and paper records.
h. Ensure records are properly stored and protected, and can easily be located and retrieved. This will include:
    i. Ensuring that adequate storage accommodation is provided for the records.
    ii. Monitoring the movement and location of records so that they can be easily retrieved and provide an audit trail.
    iii. Controlling access to the information.
    iv. Identifying vital records and applying the appropriate protection, including a business recovery plan.
    v. Ensuring non-current records are transferred in a controlled manner to a designated records centre rather than stored in offices.

In more detail; paperwork submitted to IHSGB Ltd. plus any associated documents are kept securely in lockable, non-portable cabinets with access strictly limited to IHSGB LTD. Trustees and Officers only.

If any such information is transcribed onto computer, files are protected from unauthorised access by secure user ids and passwords, and by a hardware firewall.

Where other information is received by Email, such emails are secured in a secure electronic folder with access limited to the named individual at the client organisation to whom it was addressed.

8. Record Retention and Disposal

It is important that disposal of records happens as part of a managed process and is adequately documented. We will ensure that:

a. Appropriate records are reviewed and disposed of/transferred to archive storage each year
b. Documentation of the disposal/transfer of records is completed and retained.
c. Records selected for permanent preservation are transferred to archive, as soon as possible.
d. An intended disposal/review date must be captured when creating electronic records.
e. Records subject to a Freedom of Information request are not destroyed.

Disclosing Confidential Information

Officers may not disclose information given to you in confidence by anyone, or information acquired by you which you believe, or ought reasonably to be aware, is of a confidential nature, except where:

- you have the consent of a person authorised to give it;
- you are required by law to do so;
- the disclosure is made to a third party for the purpose of obtaining professional advice provided that the third party agrees not to disclose the information to any other person; or
- the disclosure is:
  (a) in the public interest; and

(b) made in good faith and
(c) in compliance with the reasonable requirements of the Society;

What is 'confidential information'?
Information is a broad term. It includes facts, advice and opinions. It also covers written materials, including tapes, videos, CDs, DVDs and other electronic media.
Information is confidential:

- if it is about something serious and not trivial
- if the nature of the information is sensitive or personal, for example it is a business secret
- if it is information that you would expect people would want to be private
- if it was divulged in a way which implied it should be kept confidential
- if disclosing the information would be detrimental to the person who wishes to keep it confidential

If the Society, the executive or a committee of the Society has voted to treat the information as exempt, then you should maintain it as confidential.

Justification for disclosure in the public interest
Disclosing confidential information in the public interest can only be justified when **all** of the following points are met:

- **the disclosure must be reasonable** – this is a matter of judgment. However, when making this decision, you should consider carefully why you want to disclose the information, whether it is true, how serious the issue is and who to tell
- **the disclosure must be in the public interest** – information is in the public interest if:
    - a criminal offence is committed
    - the authority fails to comply with its legal obligations
    - a miscarriage of justice occurs
    - the health and safety of an individual is in danger
    - the environment is likely to be damaged
    - information about any of the issues above is deliberately concealed
- **the disclosure must be made in good faith** – the disclosure will not be justified if it is being made to promote your interests or is for political gain
- **the disclosure must be made in compliance with any reasonable requirements of your authority** – you must first raise your concerns through the appropriate channels set out in your authority's policies and procedures. For example, policies on whistle-blowing or member-officer relationships should be followed before making a disclosure.

When would a public interest disclosure not be justified?
If the disclosure would amount to a criminal offence or when information is protected by legal professional privilege, it is unlikely that its release could be justified as being in the public interest.

Policy first introduced April 2018
Author; D Ede April 2018

Adopted by IHSGB Ltd. date
Review date:
Updated :