SDS Policy on the Use of Protective Markings

Descriptor	Changes made	Date	Version
Policy first implemented	Simplified, re-structured content Revised title and wording to use protective marking instead of information classification Reviewed and Approved by Senior Dir Enabling Services	November 2019 October 2020 December 2020	1.0
Review no.1	Anticipates launch of MS sensitivity labels and their use for protective markings. Provides general definition of *SDS Confidential*. Approved A Livingstone, 9th Dec 2022	December 2022	2.0
Review no.2			

Name of policy being superseded (if applicable)	Not applicable
Related policies	Clear Desk Code of Conduct Data Protection Freedom of Information Information Access Control Records Management Using SDS IT Equipment and Systems
Related SOPs	None
Related Guidance	SDS Guide to Protective Markings SDS Guidance on How to Apply the Protective Marking to Different File Types SDS Guide to Working with Protectively Marked Information All available on Connect
Equality Impact Assessment completed	Yes.
Intended Audience	All SDS staff and contractors
Team responsible for policy	Information Governance team, within IGOR
Policy owner contact details	Kenneth Parker
Policy due for review (date)	December 2023

Contents

1. Policy summary

This policy has been written to support colleagues as they work with SDS's information by providing clear instructions on how that information should be protected and used. It will ensure that information, in whatever form and wherever it is held, is valued by the organisation, its employees and any third-party partners SDS is collaborating with.

SDS must be trusted by partners and clients as an organisation that will respect the information they share with us. Applying the correct protective marking to information and then handling it accordingly will demonstrate SDS's commitment to making sure that information receives an appropriate level of protection.

2. Policy purpose and objectives

This policy will support colleagues to work securely with SDS's information. It explains what protective markings are, how they help maintain the confidentiality of information, which markings SDS is going to use and when they should be applied to documents. It clearly sets out SDS's expectations for how information should be handled so that the confidentiality, integrity and availability of the information are adequately preserved.

Complying with the policy will demonstrate that information, in all forms and wherever it is held, is valued by SDS, its employees and any third-party partners or suppliers SDS is working with. Appropriate use of protective markings lets colleagues know the value to SDS of the information within a document and how SDS expects them to handle that document.

The policy sets out:

- What protective markings SDS is using
- When they should be applied

Further guidance on picking the appropriate protective marking in common circumstances, how to display the protective marking in common types of file and how to work with marked information is available on Connect.

3. Strategic context

Information is central to what SDS does and how it does it. Making sure that only the right people have access to the information and that they do not accidentally release it is vital to maintaining SDS's reputation and our ability to provide effective trusted public services.

SDS is working more closely with more partners than ever before and the tools within Office 365 are being used to make it easier to work with external organisations. Ease of use, however, is only one part of the answer. Staff at SDS must be able both to explain how its information should be handled by those external partners and to understand how to handle information created by an external collaborator.

4. Definitions

Protective Marking

- A label which clearly indicates the sensitivity or value of a document or piece of information

SDS Internal

- A protective marking for information whose unauthorised disclosure, particularly outside SDS, would be inappropriate.

SDS Confidential

- A protective marking for information whose unauthorised disclosure even within SDS would cause significant harm to the interests of SDS or other parties.

Descriptor

- A term used with *SDS Confidential* to describe what the nature of the sensitivity is e.g. *SDS Confidential –HR*; *SDS Confidential - Finance*.

Restricted statistics

- A marking used to protect official statistics prior to their general publication.

Sensitivity Labels

- A feature within Microsoft 365 that will help to protect SDS's information.

5. Scope

This policy applies to all SDS colleagues, regardless of the nature of their contract.
All colleagues are responsible for the success of this policy and should ensure that they take the time to read and understand it.

The scope of this policy applies to all new information, in any format, created or received by SDS.

There is no need to apply this policy to older information unless as a part of a scheduled review of that information.

6. Policy detail

The basis for this policy is that:

- Clients, partners and colleagues must be able to trust SDS with their information
- Information is an asset and has value to SDS
- Access to information will only be given to those that need to access that information for their role
- SDS must comply with statutory regulations – UK Data Protection Law and The Freedom of Information (Scotland) Act 2002

It is SDS policy on protective markings that:

- SDS will generally use one of these two protective markings -
    - SDS Internal
    - SDS Confidential – [descriptor]
- A third protective marking – *Restricted Statistics* – will be used in very particular circumstances (see below)
- The default protective marking will be SDS Internal
- Only those items which are SDS Confidential must clearly display the protective marking
- Information which is SDS Internal does not need to display the protective marking
- The person creating or receiving the information should use the issued guides to decide which protective marking is appropriate
- Sensitivity labels should be used within MS Office applications when they become available. Guidance on their use will published separately at that time.

Remember: Protective Marking - Mark to Protect

- SDS Internal - No special handling controls and no requirement to mark (routine business information)
- SDS Confidential - Protective measures or controls required (business sensitive, personal or special category information)

It is SDS policy on information handling that:

- Information must not be left unattended on desks
- Colleagues must lock their computer screens before they leave their desks unattended
- SDS Confidential information should not be printed out
- Where, exceptionally, any SDS Confidential information has been printed out, it must be locked away when not being used

- SDS Confidential information must not be sent via email outside of SDS without first being encrypted to AES 256 standard (see Guide to Working with Protectively Marked Information)
- No SDS information should be released into the public domain without its protective marking being re-assessed to ensure that no sensitive or confidential SDS information is unwittingly published.

Any colleague found to have breached this policy may be subject to disciplinary action.

SDS is a producer of official statistics for the Scottish Government. Prior to formal publication the Scottish Government requires that all such material must be marked as either *Restricted Statistics* or *Commercial Statistics*; only *Restricted Statistics* will be in use by SDS. There are specified restrictions on access to such information. If you receive material marked with *Restricted Statistics* then do not forward it on; if printing it, handle it as SDS Confidential. Further handling guidance for this class of information can be obtained from the Corporate Planning & Performance Reporting (CPPR) team.

7. Choosing the right protective marking

The protective marking must be chosen based on an assessment of the potential impact that the unauthorised publication of, or access to, the information would have on SDS, its clients or partners. The greater the projected impact then the higher the level of protective marking which must be used. For example, accidentally publishing the agenda for a team meeting might be slightly embarrassing but sending a customer's entire record to the wrong email address would almost certainly have significant reputational and financial consequences.

In general, information should be marked as *SDS Confidential* if the information could cause

- distress to an individual or group of people OR
- economic harm to a company/organisation OR
- damage to the reputation or credibility of SDS, or our partners and stakeholders

Further detail can be found in *SDS Guide to Protective Markings*, which is on Connect.

8. Using descriptors

A descriptor is a term which follows *SDS Confidential* to describe the nature of the sensitive information. Descriptors can helpful when assessing whether a colleague has a genuine business need to have access to the information. Table 8.1 provides some example descriptors but this list is not exhaustive.

Information type	**Appropriate descriptor**
Employee information	SDS CONFIDENTIAL – HR
Sensitive Partner information	SDS CONFIDENTIAL – [group/partner name] ONLY

Very Limited distribution – Named individuals	SDS CONFIDENTIAL – A Smith & B Jones ONLY

Table 8.1. Examples of descriptors.

The key here is to ensure that descriptors are used consistently across the business and that words with similar meanings are avoided. A fuller listing is provided in *SDS Guide to Protective Markings.*

Descriptors must only be used with *SDS Confidential* but a protective marking of *SDS Confidential* does not always require the use of a descriptor.

9. Further guidance

Guides have been written to help colleagues to:

- Determine the appropriate protective marking for the work they are doing
- Work with external partners when sensitive information is involved, as well as guidance on how to complete routine tasks without risk of compromising the information
- Ensure that the protective marking is visible to colleagues in different formats

These are available on **Connect.** This policy and those guides should be read along with the SDS policies on records management, data protection, information access control and the use of SDS IT equipment and systems.