Pan-Dorset Safeguarding Children Partnership

Protective Marking Guidance

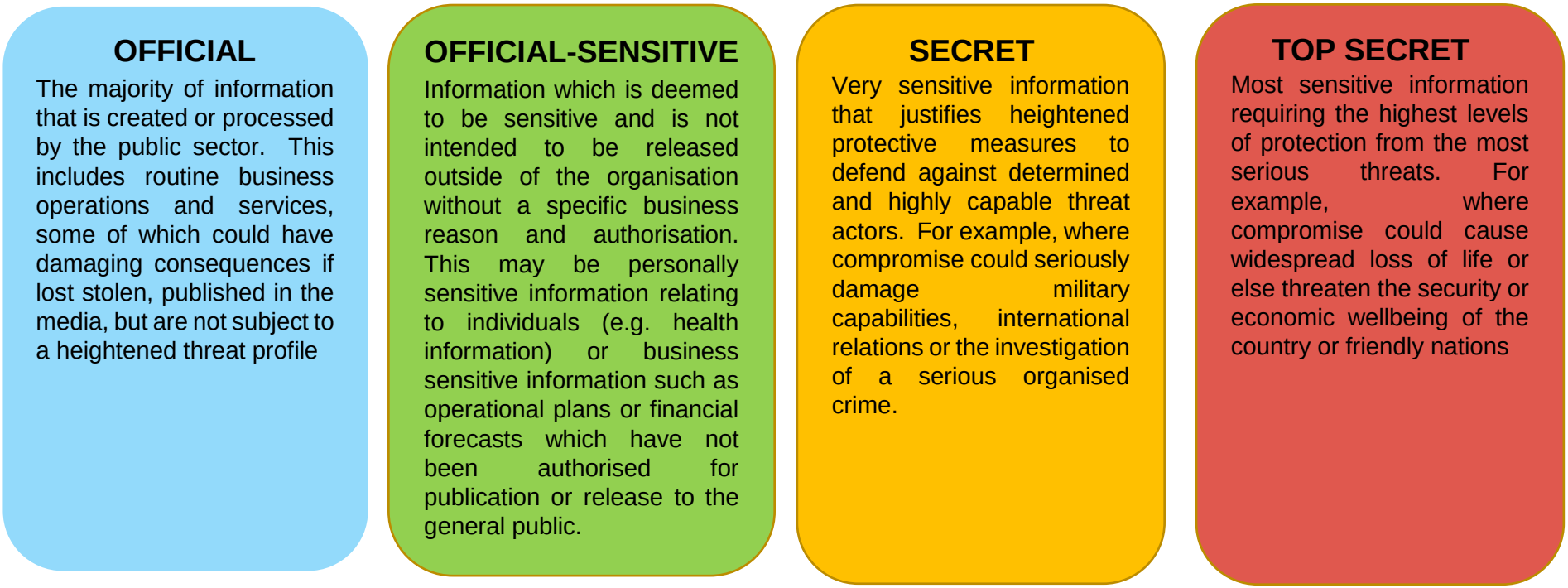
The Pan-Dorset Safeguarding Children Partnership (Pan-Dorset SCP) hold significant amounts of information, some of which is of a sensitive nature. It is important that at any time the level of sensitively of a document can be easily and accurately understood by those handling it. This is achieved by the use of protective markings.

1 What are Protective Markings?

1.1 All documents must be considered as to whether they should be protectively marked in accordance with the sensitivity of their content. This principle should also apply to documents used within the Pan-Dorset SCP and with its partners. The protective marking of a document provides people with information on the following aspects of the document:

- The correct level of protection the document should be given;
- The procedures to be followed regarding the production, dispatch, receipt, handling and destruction of the document;
- The severity or impact of the loss or compromise of the document.

1.2 The UK Government has 3 levels of protective marking: **TOP SECRET**, **SECRET** and **OFFICIAL**. The **TOP SECRET** and **SECRET** categories only apply to central government.



1.3 All Pan-Dorset SCP information falls under the classification of **OFFICIAL**.

1.4 However, there is no requirement to explicitly mark routine OFFICIAL information.

1.5 Additional measures need to be taken for the Pan-Dorset SCP's sensitive information with the use of an additional descriptor of OFFICIAL-SENSITIVE

2. How to apply the protective Marking?

2.1 Information that originates from outside of the Pan-Dorset SCP may not be protectively marked. If it is received by the Pan-Dorset SCP and it is of an OFFICIAL-SENSITIVE nature there is no onus on the Pan-Dorset SCP to mark it as long as the data is handled appropriately. However, in some circumstances the Pan-Dorset SCP may wish to mark such documents as 'OFFICIAL-SENSITIVE' to ensure the correct level of protection is given to the document.

2.2 Information received by the Pan-Dorset SCP which already has a recognised protective marking should be respected and held in line with that protective marking.

2.3 Information that is marked with a marking that is not recognised should be assessed and regard must be had to the sensitivity of the document. For example, documents may be received that are marked "private and confidential". It is advisable that such documents should be assessed in accordance with the sensitivity of the information and whether it is information that is truly either private or confidential in nature. Consideration should be given whether such documents should be marked "OFFICIAL-SENSITIVE" by default.

Official (no need to mark)	Official - Sensitive
• Any published data • Publicity material • Annual reports • Draft letters (depending on content) • Pan-Dorset SCP agenda papers and Minutes (apart from exemptions) • Team/Department agenda papers • Advice to members • Policy formulation (depending on content)	• Rapid Review Information • Child Safeguarding Practice Review Information • Domestic Homicide Review information • Complaints containing sensitive personal information • Multi and Single Agency Audit reports • Child Death information • Pan-Dorset SCP Personnel files and papers

3. Roles and responsibilities

3.1 **Originator**. The originator of a document (or any other format of information) is responsible for setting the protective marking of the particular document / information (digital or paper) at the initial stage of document creation. Over time it might be necessary to change the protective marking of a document which is also a responsibility of the originator when known or approved by the Pan-Dorset SCP Business Manager if the provenance of the decision is unknown. This may include external documents that were unmarked when they were received and marked up internally to comply with the Protective Marking Policy.

3.2 **User/keeper**: All Pan-Dorset SCP members in possession of information with a protective marking are responsible for handling the information in accordance with this marking. This includes storing, processing, sharing and destroying.

4. Handling OFFICIAL/OFFICIAL-SENSITIVE information

The following table lists different data formats and how such documents need to be handled if they are of a sensitive nature:

Formats	OFFICIAL Procedure	OFFICIAL - SENSITIVE Procedure
MSOffice documents	Normal use of documents. There is no need to mark the document OFFICIAL.	All OFFICIAL - SENSITIVE electronic documents should be protectively marked with the appropriate security level displayed in the designated part of the document; the title page of the document (if there is one) and also in the header or footer of the document.
Emails sent internally or externally	Normal use of Email system.	OFFICIAL - SENSITIVE emails should be sent by secure email or encrypted before sending. This includes also when sending documents that have the OFFICIAL – SENSITIVE marking.

Formats	OFFICIAL Procedure	OFFICIAL - SENSITIVE Procedure
Faxing	Normal use of a fax machine. There is no need to mark the fax OFFICIAL.	The use of fax machines should be discouraged. However, if sensitive faxes have to be sent then it should be protectively marked with the security level OFFICIAL - SENSITIVE on the lead sheet and also in the top left hand corner of each page. One touch dialling **must not** be used in case the number has been changed or corrupted. Only send once, either confirm with the intended recipient that they are able to collect the fax immediately or the receiving fax is known to be in a secure environment.
Database reports	Normal use of documents. There is no need to mark the report OFFICIAL.	Much information is produced or created from databases or reporting software, this must all be marked using the same method as above. A database which consists largely of OFFICIAL - SENSITIVE data may produce reports or statistics which are not sensitive, so it is not possible to conclude that all the reports produced from sensitive databases are in themselves sensitive; some applications enable desensitised reports to be produced. Any sensitive documents printed or electronically copied should be marked OFFICIAL - SENSITIVE in the header of the document.
Files, Printed material	Normal use of documents. There is no need to mark the material OFFICIAL.	All files, folders and printed materials must have their security classification boldly displayed on the front of the file or folder. Documents should be marked OFFICIAL - SENSITIVE in the header or footer of the document. The owner of the document must be specified so the document may be returned correctly.
Letters, post etc	Post as per normal procedures. There is no need to mark the letter OFFICIAL, though the letter templates have been set up with an OFFICIAL marking.	Letters should be marked in the top left hand corner with OFFICIAL - SENSITIVE. National guidelines recommend that such letters or packages (containing files) should:

Formats	OFFICIAL Procedure	OFFICIAL - SENSITIVE Procedure
		• Mark for the attention of and include return address – if this is wrongly addressed return to… Never mark classification on envelope. • Consider double envelope for sensitive assets • Consider using registered Royal Mail service or reputable commercial courier's 'track and trace' service However, it is recognised that this can be expensive and difficult to do (e.g. the mail room machines are not designed for double enveloping). A compromise position would be to send the letter as normal making sure that it is appropriately marked in the header of the letter but NOT marking the outer envelope. This will mean that the sensitive nature of the content is protected **BUT** it will mean that the person opening the letter **will not** be aware of the sensitive nature that an inner marked envelope would bring.
Storage		Store OFFICIAL - SENSITIVE assets under lock and key
Disposal / Destruction		• Dispose of information with care • For paper ensure data is shredded or destroyed as per approved commercial contract • Electronic information within our systems need to be disposed of in compliance with agreed retention periods • IT hardware needs to be disposed of as per our approved commercial contract • Destruction dates to be agreed

5. Retention of records

Important Note: The Independent Inquiry into Child Sexual Abuse requires all institutions to retain their records relating to the care of children for the duration of the Inquiry under Section 21 of the **Inquiries Act 2005**. There is therefore an obligation to preserve records for the Inquiry for as long as is necessary. For the Pan-Dorset SCP this will apply to any child-specific information. When this requirement is lifted a schedule of retention will be re-instated by the Pan-Dorset SCP.

(See letter to **Chief Executives of Local Authorities**).

6. Legal Framework

The UK classification system operates within the framework of domestic law. This includes:

a. **Official Secrets Act 1989**: Damage assessment is a critical element of the OSA, most of the offences in which require there to have been a damaging disclosure of information relating to security or intelligence, defence, international relations, crime or special investigation powers, or of confidential information received from a foreign State or an international organisation. With respect to each type of information, the OSA describes the type of damage which has, or would be likely, to flow from an unauthorised disclosure. The OSA also specifies who is capable of committing offences under it. Different offences apply to: members of the security and intelligence services; persons notified under section 1 of the OSA; Crown servants; government contractors; and any person.

b. **Data Protection Legislation**: The handling of personal data must be in compliance with Data Protection legislation. The Data Protection Act 2018, however, contains a number of exemptions to some or all of the data protection principles and to other provisions such as the right of access to personal data. For example, the Act provides an exemption from many of the requirements of the Applied General Data Protection Regulation to safeguard national security. But note that, although the exemption is widely drawn, it is only available to the extent that it is required for the purpose of protecting national security. Thus departments and agencies will still be required to assess whether it is possible to address national security concerns and comply with Data Protection legislation. Whilst the presence or absence of a classification marking is not in itself a deciding factor as to whether an exemption is engaged, it may be a helpful indicator that one

applies. Departments and agencies should also have regard to Data Protection legislation, including any relevant exemptions, when sharing personal data with other departments and agencies or pursuant to international agreements.

c. **Freedom of Information Act 2000**: Classification markings can assist in assessing whether exemptions to the Freedom of Information Act 2000 (FOIA) may apply. However, it must be noted that each FOI request must be considered on its own merits and the classification in itself is not a justifiable reason for exemption. It is therefore important that staff (including contractors) who handle, or are likely to handle sensitive assets, understand fully the impact of such legislation and how it relates to their role.

d. **Public Records Act 1967**. Records selected for preservation may be retained under Section 3(4) of the 1958 Act or closed under an exemption provided by the Freedom of Information Act 2000. Decisions over retention or closure are driven by perception of residual sensitivities at the time that release is being contemplated.