# MELTON BOROUGH COUNCIL

# PROTECTIVE MARKING SCHEME

# PROTECTIVE MARKING SCHEME: CONTENTS

# 1. Introduction

This Protective Marking Scheme document sets out the aims, objectives, standards, and overall approach to protective marking by Melton Borough Council.

The Protective Marking Scheme helps to ensure that the Council's use of information assets both reflects and complies with central government best practice in this area of work.

Protective marking can apply to buildings and computers, for example, as well as electronically-held information or paper documents.

# 2. Aims and Objectives

The ultimate aim of a protective marking scheme is to provide for a controlled, risk managed and safe system for rating and handling the sensitivity of information assets.

The objectives of a protective marking scheme are as follows:-

- To provide for a formal mechanism to enable information assets to be classified.
- To provide sufficient guidance to officers of the Council to enable them to mark the information assets appropriately.
- To provide a system for the management of information risk in relation to information assets.
- To provide a system for the handling of breaches of the protective marking scheme.

# 3. Background

The Council Protective Marking Scheme is derived from the Government Security Classifications Policy (GSCP).

The Government system includes a number of levels of protective marking which would ***not*** be considered to apply to information assets at a purely local government level. The ***non-applying*** levels would be TOP SECRET and SECRET.

Levels that ***could apply*** to local authority activity would be considered to include the marking of OFFICIAL.

The previous designations of PROTECT and RESTRICTED can both be used as subdivisions of OFFICIAL for practical purposes, as former RESTRICTED items have greater severity in relation to Business Impact Levels (BILs), so PROTECT = OFFICIAL, RESTRICTED = OFFICIAL (SENSITIVE).

The Government Security Classifications Policy is closely connected with standard classifications of Business Impact Levels (BILs) on defined areas of public business in the United Kingdom.

For Melton Borough Council, the protective marking levels can be explicitly mapped to its existing risk matrix covering risks related to disclosure of information handled through its Information Sharing Policy and Guidance.

## 4. The Protective Marking Scheme

The Council's Scheme, fitted within the national framework, comprises **one** of the three national markings. In descending order of sensitivity, this is:

**OFFICIAL**

**and should be subdivided to distinguish the former categories of PROTECT and RESTRICTED: OFFICIAL and OFFICIAL (SENSITIVE)**

Unmarked material is considered 'unclassified'. These markings can be applied to any Council assets, although they would be most commonly applied to information held electronically or in paper documents.

**Universal controls**
There are a number of specified technical controls for each level of protective marking. The controls below apply to all protectively marked information.

**The following baseline controls must apply to all protectively marked material:**

a. Access is granted on a genuine 'need to know' basis.
b. Assets must be clearly and conspicuously marked. Where this is not practical (for example the asset is a building, computer, etc) staff must still have the appropriate personnel security control and be made aware of the protection and controls required.
c. Only the originator or designated owner can protectively mark an asset. Any change to the protective marking requires the originator or designated owner's permission. If they cannot be traced, a marking may be changed, but only by consensus with other key recipients. At Melton, this would mean approval by the Information Management Group and the Council's Monitoring Officer.
d. Assets sent overseas (including to UK posts) must be protected as indicated by the originator's marking and in accordance with any international agreement.
e. No official record, held on any media, can be destroyed unless it has been formally reviewed for historical interest under the provisions of the Public Records Act.
f. A file, or group of protectively marked documents or assets, must carry the protective marking of the highest marked document or asset contained within it (eg, a file containing OFFICIAL (SENSITIVE) and OFFICIAL material must be marked OFFICIAL (SENSITIVE)).

**Applying the correct protective marking**
The originator or nominated owner of information, or an asset, is responsible for applying the correct protective marking. When protectively marking a document, it is recommended that a damage or 'harm test' is conducted to consider the likely impact if the asset were to be compromised and to help determine the correct level of

marking required. The 'harm test' should be done by assessing the asset against the criteria for each protective marking.

If applied correctly, the Protective Marking Scheme will ensure that only genuinely sensitive material is safeguarded. This should assist Council Officers in determining those items that would be exempt from disclosure in information requests under the Freedom of Information Act 2000 or the Environmental Information Regulations 2004.

The following points should be considered when applying a protective marking:

- Applying too high a protective marking can inhibit access, lead to unnecessary and expensive protective controls and impair the efficiency of an organisation's business.
- Applying too low a protective marking may lead to damaging consequences and compromise of an asset.
- The compromise of aggregated or accumulated information of the same protective marking is likely to have a higher impact (particularly in relation to personal data):
    - Generally this will not result in a higher protective marking but may require additional handling arrangements.
    - However, if the accumulation of that data results in a more sensitive asset being created, then a higher protective marking should be considered.
- The sensitivity of an asset may change over time, and it may be necessary to reclassify assets. If a document is being de-classified or the marking changed, the file should also be changed to reflect the highest marking within its contents.

The criteria below provide a broad indication of the type of material at each level of protective marking.

**Table 4.1 Central Government Categories**

| **Criteria for assessing OFFICIAL (SENSITIVE) assets:** |
|---|
| Affect diplomatic relations adversely;<br>Cause substantial distress to individuals;<br>Make it more difficult to maintain the operational effectiveness or security of United Kingdom or allied forces;<br>Cause financial loss or loss of earning potential or to facilitate improper gain or advantage for individuals or companies;<br>Prejudice the investigation or facilitate the commissioning of crime;<br>Breach proper undertakings to maintain the confidence of information provided by third parties;<br>Impede the effective development or operation of government policies;<br>To breach statutory restrictions on disclosure of information;<br>Disadvantage government in commercial or policy negotiations with others;<br>Undermine the proper management of the public sector and its operations. |
| **Criteria for assessing OFFICIAL assets:** |
| Cause distress to individuals;<br>Breach proper undertakings to maintain the confidence of information provided by third parties;<br>Breach statutory restrictions on the disclosure of information; |

| |
|---|
| Cause financial loss or loss of earning potential, or to facilitate improper gain;<br>Unfair advantage for individuals or companies;<br>Prejudice the investigation or facilitate the commission of crime;<br>Disadvantage government in commercial or policy negotiations with others. |

It can be clearly seen that the OFFICIAL level is explicitly provided for sub-national information asset marking, but the Council does have some areas of work which would impact at a national level, and where OFFICIAL (SENSITIVE) might be appropriate:

- Crime and disorder policy and work, including criminal investigations
- Business issues with market impacts, such as Government – City Deal negotiations
- Emergency planning
- Defence assets within the Borough
- Large personal data transfers to national level organisations, such as the Department of Work and Pensions (DWP), where data protection breaches might facilitate serious organised crime.

## 5. Breaches

The Council must present its staff with a clear indication of the incremental penalties for breaching the rules regarding protectively marked material and the other mandatory requirements as laid out in this Scheme. This must include recourse to disciplinary and, where applicable, criminal proceedings.

**There must be a breach system and clear guidance given to all staff and Elected Members that deliberate or accidental compromise of protectively marked material may lead to disciplinary and or criminal proceedings.**

### 5.1 Breach Procedure

The procedure for handling breaches relating to protectively marked information assets is essentially that set out in the Parkside Multi-agency Information Incident Handling documentation. This is available from the Parkside Intranet page.

Elected Members should follow the same process, and report any breaches they are aware of to one of the named Information Managers for Melton Borough Council in the documentation, having completed a breach form as set out in the Handling Procedure.

### 5.2 Breach Guidance for Council Staff

Deliberate or negligent compromise of protectively marked material by Council staff could constitute a serious breach of confidence within the meaning of gross misconduct at paragraph 4.2 of the Council's Disciplinary Procedure (February 2010 version). Proportionality would require that the establishment of mitigating circumstances in the case of a genuine accident would occasion a different outcome from a deliberate act of unauthorised disclosure, or a negligent act leading to unauthorised disclosure.

A deliberate act of unauthorised disclosure with a public interest defence would be contested by the Council, as the establishment of public interest in the Council's protectively marked information assets would be reserved to the Information Management Group and sign-off by the Council's Qualified Person as defined in the

Ministry of Justice Guidance on Section 36 of the Freedom of Information Act 2000. Any member of Council staff who considers that a protectively marked information asset should be declassified and made disclosable in the public interest should refer the matter to their Head of Service, so that a public interest test can be undertaken by the IMG, and signed off by the Council's Qualified Person.

**5.3 Breach Guidance for Elected Members**

Deliberate or negligent compromise of protectively marked material by Elected Members, that resulted in a complaint, could constitute a serious breach of confidence, and prohibition on disclosure would fall within the meaning of the Members' Code of Conduct Section 4.

A deliberate act of unauthorised disclosure, or a negligent act leading to unauthorised disclosure, that resulted in a complaint, may fall within the meaning of the Members' Code of Conduct Section 5, relating to conduct which could reasonably be regarded as bringing that Elected Member's office or the Council into disrepute.

A deliberate act, by an Elected Member, of unauthorised disclosure with a public interest defence would be contested by the Council, as the establishment of public interest in the Council's protectively marked information assets would be reserved to the Information Management Group and sign-off by the Council's Qualified Person as defined in the Ministry of Justice Guidance on Section 36 of the Freedom of Information Act 2000. Any Elected Member who considers that a protectively marked information asset should be declassified and made disclosable in the public interest should refer the matter to the Council's Monitoring Officer, so that a public interest test can be undertaken by the IMG, and signed off by the Council's Qualified Person.

The adoption of a process for determining public interest which draws on a shared organisational understanding, professional expertise, case law and precedent, helps to protect both the Council's staff and Elected Members from suggestions of self-interest and individual bias, or perceptions of 'maverick' or 'self-appointed' interpretations of public interest.

**5.4 Criminal penalties**

Unauthorised disclosures of protectively marked information assets may constitute criminal offences, where these lead to breaches of law, such as those under Section 55 of the Data Protection Act 1998, for example. These penalties would apply both to those making deliberate unauthorised disclosures and to anyone procuring such a disclosure.

## 6. Information Risk Rating

Melton Borough Council already rates information risk in relation to information incidents that could arise concerning the information it holds, and information it holds in conjunction with its partner organisations. This is covered in the Multi-agency Incident Handling Procedure documentation.

The risk table in the Multi-agency Incident Handling Procedure documentation is extended, in relation to Protectively Marked material and in relation to Business Impact Levels (BILs) in the HMG IA Standard No. 1 Business Impact Level Table 4 for Public Services, shown below:

**Table 6.1**

| ***Severity Type*** | ***Severity Rating*** | | | |
|---|---|---|---|---|
| | ***None/ Negligible*** | ***Marginal*** | ***Significant*** | ***Severe*** |
| | **A - Green** | **B - Yellow** | **C - Orange** | **D - Red** |
| | **No ICO referral** | **No ICO referral** | **Refer to ICO – may involve some partners** | **Refer to ICO – involves all partners** |
| **MBC Risk Management matrix value** | *MBC Risk rating C1: Significant Probability, Negligible Impact* | *MBC Risk rating C2: Significant Probability, Marginal Impact* | *MBC Risk rating C3: Significant Probability, Critical Impact* | *MBC Risk rating C4: Significant Probability, Catastrophic Impact* |
| **Protective Marking – mapped to risk of disclosure** | [Not Protected] | [Not Protected] | **OFFICIAL** level | **OFFICIAL (SENSITIVE)** level |
| **Business Impact Level (BIL)** | BIL 0 | BIL 1 | **BIL 2, 3** | **BIL 4, 5, 6** |
| **A. Risk to individual(s) safety** | None/ Negligible | | Any risk to personal safety | Threatens life |
| **B. Distress caused to any party (service user, employee, visitor) including party's reputation** | None/ Negligible | Minor local impact and/or short term distress/ damage | Limited long term distress/ damage | Substantial long term distress/ damage |
| **C. Co-located Partners affected** | | Small area/Most areas within a single Partner | Multiple co-located Partners | All co-located Partners |
| **D. Adverse publicity, complaints, breach of legal/statutory requirements, risk of litigation** | None/ Negligible | Minor local impact, no risk/low risk short term of adverse publicity and/or risk litigation | Moderate/ significant damage due to adverse publicity and multiple complaints | Severe adverse publicity, breach of legal/statutory requirements, high risk of litigation |
| **E. Disruption to partner(s) business operations or service delivery** | None/ Negligible | Minor interruptions or delays | Partner business operations impaired in any way, or loss of completed transactions/transactions in progress | Partner business halted and unable to continue to deliver service |
| **F. Unauthorised disclosure of personal or commercially sensitive information** | None or Negligible disclosure of sensitive information | Minor Impact | Measurable/ significant impact to person, partner or business/breach of regulations | Substantial impact to person, partner or business |
| **G. Financial loss to any client of the service provider or 3rd party** | None/ Negligible <£100 | Minor loss < £500 | Moderate Loss < £1000/Significant Loss < £3000 | Substantial Loss > £3000 |

| | | | | |
|---|---|---|---|---|
| **H. Assistance to crime or impact on its detection** | Would be of no or negligible assistance or hindrance to detection of unlawful activity | | Prejudice investigation/ impede investigation or assist in a crime | Prevent investigation or directly assist serious crime |

The Business Impact Level Table 4 for Public Services is **Annexe 1** to this Scheme document.

## 7. Process for Council Officers

The information asset owner should consider the information asset (document, etc) that is to be assigned a protective marking.

(i) Check the BIL table (**Annexe 1**).
(ii) Assess the BIL that applies, looking at the information in the table.
(iii) Look at the ***criteria*** for OFFICIAL (SENSITIVE) and OFFICIAL (**Table 4.1**).
(iv) Check the mapping of BIL, protective marking level and MBC Risk Management matrix value and disclosure risk (**Table 6.1**).
(v) Assign a protective marking level, or leave unmarked, as appropriate.
(vi) If a protective marking level is to be applied to a document, the document should be converted to PDF once the level has been applied, so that the marking cannot be tampered with.
(vii) Keep a record of the decision you have made and the BIL that applies to the information asset if a protective marking level is applied.
(viii) The information asset owner should notify the Information Management Group of the BIL and the protective marking level applied, in case a review of the marking level is necessary.

## 8. Document ownership and change control

This Protective Marking Scheme document is owned by the Corporate Management Team. The Scheme will be maintained by the Council's Monitoring Officer and the Information Management Group, who will assess feedback on the process and progress any identified request for change.