Information Classification and Handling Policy

<table>
<thead>
<tr>
<th>Document title</th>
<th>Information Classification and Handling Policy</th>
</tr>
</thead>
<tbody>
<tr>
<td>Summary of purpose</td>
<td>This policy defines the Information Classification and Handling Policy and is in support of the Corporate Information Security Policy.</td>
</tr>
<tr>
<td>Prepared by (document owner)</td>
<td>Ray Ware, IT Manager</td>
</tr>
<tr>
<td>Status</td>
<td>Revision</td>
</tr>
<tr>
<td>Version number</td>
<td>V3.0</td>
</tr>
<tr>
<td>Approved by</td>
<td>Full Council</td>
</tr>
<tr>
<td>Approval date</td>
<td>13 Sept.2013</td>
</tr>
<tr>
<td>Date of implementation</td>
<td>1st October 2013</td>
</tr>
<tr>
<td>Review frequency</td>
<td>On significant change dictated by external factors</td>
</tr>
<tr>
<td>Next review date</td>
<td></td>
</tr>
<tr>
<td>Published on the Council’s website</td>
<td>No</td>
</tr>
</tbody>
</table>

Validity Statement

This document is due for review by the date shown above, after which it may become invalid. Users of this policy or strategy should ensure that they are consulting the currently valid version of the document.
PART 1 – General Principles

1 Introduction
This policy defines the Information Classification and Handling Policy and is in support of the Corporate Information Security Policy.

2 Definitions
- Information Classification is a scheme that is very discretionary and varies between organisations.
- The Information Classification scheme is used to determine how to separate, where necessary, the information into differing levels of sensitivity based on levels of confidentiality and integrity required by the owner, and allow the access control policy to be applied to sections of information based on the varying levels of sensitivity.
- “User” refers to any employee, elected member, agency worker, third party organisation or other authorised personnel.
- “Service Users” refers to all individuals who use the service of an Organisation and whose sensitive information may be held by the authority.
- “Information Owners” are the Heads of Service and their Managers responsible for the information contained within the service areas.
- “Information” is all Maldon District Councils information, information owned by its suppliers, partners and clients, and information about its Service Users, in whatever form it may be held and however it may be stored, processed or communicated.

3 Scope
This policy applies to all users.

4 Authority
This policy is supported by the Chief Executive of Maldon District Council

5 Objectives
The objective of the Information Classification and Handling Policy is:
- To provide guidance on handling information of each classification in different circumstances and locations including creation, modification or processing, storage, communication, retention and deletion, disposal or destruction.

6 Roles and responsibilities
- Information owners will be responsible for defining the value of information, and identifying the risks associated with the information, so they must classify their information, and define the controls for its protection.
7 Policy statements

7.1 Information Classification and Handling
7.1.1 All information must be handled in accordance with the Councils Information Classification Scheme.
7.1.2 All confidential information must only be accessible on a need-to-know basis.
7.1.3 Personal information held as hard copy should be disposed of by incineration, pulping or shredding, and that held on electronic media by overwriting, erasure or de-gaussing for re-use using CCTM approved products or services for preference.
7.1.4 All transfers of personal data from the organisation to countries outside of the EEA (European Economic Area) must be risk assessed and must be fully compliant with all data protection requirements.
7.1.5 Information Owners should regularly review user access rights and amend if appropriate.
7.1.6 The Council should develop and execute plans to lead and foster a culture that values, protects and uses information for the public good.
7.1.7 Mechanisms through which individuals may raise concerns about information risk to the attention of senior management should be in place.
7.1.8 The Councils Information Owners should continually enhance the use of information assets within the boundaries of the law.
7.1.9 The Council should continually enhance public protection and public services through greater access to information held by others within the boundaries of the law.
7.1.10 The Council should publish an information charter setting out how it handles information and how members of the public can address any concerns that they might have.
7.1.11 The bulk transfer of information should be done electronically across the secure corporate network.
7.1.12 Information being shared between organisations should make use of the Essextranet or PSN network as applicable
7.1.13 Suppliers or contractors handling information on behalf of the Council should operate under equivalent standards to those applied to members and Officers of the Council

PART 2 – Additional Requirements

8. Maldon District Council Specifics

8.1 Information Classification Scheme – up to 31st March 2014
8.1.1 As an active participant in the EssexOnline Partnership the Council has been working to produce a pan-Essex Information Classification Scheme which will define specific Classification for each record type in line with the Local Government Classification Scheme.
8.1.2 The combined force of the Data Protection Act and Data Handling Procedures in Government make it critical for Councils to recognise the sensitive data they hold and apply appropriate levels of protection to it. To ensure a uniform method of assessing the impact of potential compromises to the confidentiality, integrity or availability of
information and information systems, and provide comparable levels of information protection when the data is shared, Business Impact Levels tables have been devised which reflect the potential levels of distress to the Public. For example,

<table>
<thead>
<tr>
<th>Level 1</th>
<th>Level 2</th>
<th>Level 3</th>
<th>Level 4</th>
<th>Level 5</th>
<th>Level 6</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td>Likely to cause embarrassment to an individual or organisation</td>
<td>Likely to cause loss of reputation to an individual or organisation</td>
<td>Likely to cause embarrassment or loss of reputation to many citizens or organisations</td>
<td>Likely to cause long term (eg months) or permanent loss of reputation to many citizens or organisations</td>
<td>Likely to cause major long term damage to the UK population</td>
</tr>
</tbody>
</table>

8.1.3 All data – electronic or on paper – should be labelled according to the protection it requires, based on these Impact Levels. Document classification categories are shown in the following table;

<table>
<thead>
<tr>
<th>Impact Level</th>
<th>Document Classification</th>
</tr>
</thead>
<tbody>
<tr>
<td>IL0</td>
<td>equivalent to Unclassified / Not Protectively Marked</td>
</tr>
<tr>
<td>IL1</td>
<td>equivalent to Protected</td>
</tr>
<tr>
<td>IL2</td>
<td>equivalent to Protected</td>
</tr>
<tr>
<td>IL3</td>
<td>equivalent to Restricted</td>
</tr>
<tr>
<td>IL4</td>
<td>equivalent to Confidential</td>
</tr>
<tr>
<td>IL5</td>
<td>equivalent to Secret</td>
</tr>
<tr>
<td>IL6</td>
<td>equivalent to Top Secret</td>
</tr>
</tbody>
</table>

The highest security class the Council is likely to have to deal with in daily operations is Restricted – IL3. Confidential, Secret and Top Secret classifications are highly unlikely to apply to any correspondence we come across and are mainly utilised within the MoD and other Central Governmental departments.

8.2 Document Handling – Current Scheme

8.2.1 UNCLASSIFIED - These documents are available for general consumption. They contain no information that may be classified as “personal” and may be stored in any location. Members and Officers must still exercise caution in the handling of these documents, but no special data handling requirements exist.

8.2.2 PROTECTED - These documents contain personal information relating to a client, partner organisation or other correspondent which require a degree of confidentiality. Protected documents should be stored in secure physical locations if hard copy (ie: locked
cupboards or drawers when not actively being utilised), or in secure file structures if
electronic. In both cases access must be restricted to specified individuals. A full
electronic audit trail will be maintained of all access to these documents, and they must
be encrypted when stored on removable media or mobile devices.

8.2.3 RESTRICTED - These documents are the highest Impact Level the Council is likely to
handle. They should not be forwarded to any other recipient. Hard copy must be treated
as per Protected but may require even tighter security over access depending on the
content. Electronic copies may only be stored in a dedicated secure location with full
electronic auditing enabled.

8.2.4 The main difference between handling PROTECTED and RESTRICTED protectively
marked documents is that Members and Officers may discuss the contents of
PROTECTED documents over the telephone, but may not do the same for RESTRICTED
documents whose contents are strictly confidential to the addressee only.

8.3 Information Classification Scheme – from 1st April 2014

8.3.1 From 1st April 2014, the Governments security arm (CESG) will be reducing the number
of classifications from 7 to 3, these being Official, Secret and Top Secret. There is no
direct correlation between the new scheme and the existing Protective Marking Scheme.

8.3.2 The vast majority of transactions and correspondence undertaken within Local
Government will fall under the Official category, and the Government have pointed out
that there is a very significant step up (described as a “Cliff Face”) between this and the
Secret classification. It is therefore highly unlikely that any transactions or
correspondence undertaken by Maldon District Council will fall into either of the higher
two categories.

8.3.3 For this reason there is no longer a requirement to protectively mark documents from the
date this scheme becomes effective.

8.3.4 Further details regarding this scheme together with a useful FAQ document can be found
on the Cabinet Office Website.

8.4 Document Handling – New Scheme

8.4.1 The apparent relaxation in Protective Marking reflects Government acceptance that there
are already sufficient legislative and procedural requirements in existence to safeguard
Public Sector Information Assets (eg: Data Protection Act, specific legislation relating to
service delivery etc.).

8.4.2 Information Owners have a duty to ensure that all Maldon District Council data assets are
managed, safeguarded and secured in line with this legislation. It is the individual
Information Owners responsibility to maintain a register of those Information Assets that
he/she is responsible for, and to record and manage the risks associated with those
assets accordingly.

8.4.3 The Councils Organisational Development team will collate these individual registers to
form a comprehensive corporate register of information assets and risks to ensure
consistency across the organisation.

8.4.4 Requests for further information or queries relating to the handling or classification of
information should be directed to the Councils SIRO, Peter Wyatt, Head of Organisational
Development.
9 Documentation

Document Authors: Essex OnLine Partnership Resource Team and Maldon District Council
Disclaimer: This printed version may not be the current version. A current version may be obtained from the EOLP Resource Team or Maldon District Councils ICT Manager

Version History

<table>
<thead>
<tr>
<th>Version No</th>
<th>Release Date</th>
<th>Update Authorised by</th>
<th>Update carried out by</th>
<th>Update Approved by</th>
<th>Changes</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.1</td>
<td>March 2008</td>
<td>EOLP</td>
<td>EOLP Resource Team</td>
<td></td>
<td>First draft</td>
</tr>
<tr>
<td>0.2</td>
<td>March 2008</td>
<td>EOLP</td>
<td>EOLP Resource Team</td>
<td>EOLP Information Security Working Group</td>
<td>Changes agreed or adjusted following Hytec recommendations by the EOLP Information Security working group on 10-03-08</td>
</tr>
<tr>
<td>1.0</td>
<td>28th March 2008</td>
<td>EOLP</td>
<td>EOLP Resource Team</td>
<td>EOLP Information Security Working Group</td>
<td>Changes agreed by the EOLP Information Security working group on 17-03-08.</td>
</tr>
<tr>
<td>1.1</td>
<td>11th April 2008</td>
<td>Ray Ware</td>
<td>Ray Ware</td>
<td></td>
<td>Tailored to MDC requirements for consideration by OPPB</td>
</tr>
<tr>
<td>1.2</td>
<td>3rd February 2009</td>
<td>Ray Ware</td>
<td>Ray Ware</td>
<td>CMT F&amp;CS</td>
<td>Amended to reflect GC and LGA Data Handling Guidance requirements Approved by CMT 03/03/09 Approved by F&amp;CS 14/04/09</td>
</tr>
<tr>
<td>2.0</td>
<td>18th May 2009</td>
<td>N/A</td>
<td>Ray Ware</td>
<td>Council</td>
<td>Policy adopted by Council on 07/05/09</td>
</tr>
<tr>
<td>3.0</td>
<td>1st October 2013</td>
<td>F&amp;CS 23/07/13</td>
<td>Ray Ware, IT Manager</td>
<td></td>
<td>Inclusion of PSN references and re-written for new scheme.</td>
</tr>
</tbody>
</table>