Inverclyde council

**AGENDA ITEM NO: 15**

| | | | |
|---|---|---|---|
| **Report To:** | **Policy and Resources Committee** | **Date:** | **19 September 2017** |
| **Report By:** | **Louise Long<br>Corporate Director (Chief Officer)<br>Inverclyde HSCP** | **Report No:** | **PR/21/15/DR** |
| **Contact Officer:** | **Dean Robinson<br>Information Governance Officer** | **Contact No:** | **01475 712136** |
| **Subject:** | **INFORMATION CLASSIFICATION POLICY IMPLEMENTATION** | | |

## 1.0 PURPOSE

1.1 The purpose of this report is to report back to the Committee on the implementation of the Information Classification Policy.

## 2.0 SUMMARY

2.1 The Information Classification Policy was approved at the Policy and Resources Committee on 22 September 2015.

2.2 The Policy enforces the protective marking with a security classification to all forms of information both hard copy (paper) and electronic data including e-mail, and all magnetic media, which includes CD ROMs, hard drives, removable hard drives originating within Inverclyde Council.

2.3 Implementation of the Policy will be in the form of raising its awareness amongst staff and includes a software tool, training and guidance on how to classify information.

2.4 The Council through the Information Governance Steering Group (IGSG) has embarked on the following steps to enforce and implement the Policy:

- Email labelling and classification software tool;
- Protective Marking, Sharing and Disclosing Information E-learning module;
- An Implementation Guide to be used in conjunction with the Policy;
- Awareness raising communications.

Once these tools have been fully deployed, services will be notified that they will be available with user guidance where appropriate to ensure that implementation of the Policy is adhered to.

## 3.0 RECOMMENDATIONS

3.1 It is recommended that the Committee:

a) Note the steps being taken in this report to enforce and implement the Information Classification Policy.

**Louise Long**
**Corporate Director (Chief Officer)**
**Inverclyde HSCP**

## 4.0 BACKGROUND

4.1 The Information Classification Policy was first submitted to the Policy & Resources Committee on 13 August 2013. The Policy presents a common approach to information classification and guidance for all services to use and assist them in establishing effective information classification practices.

4.2 Following changes to the UK Government Security Classifications in 2015, an updated Policy reflecting these changes was presented to the Committee on 22 September 2015. The updated Policy presents a more simplified approach of having fewer levels of security classifications suited to more modern workplaces and electronic information. Inverclyde Council has adopted the OFFICIAL and OFFICIAL-SENSITIVE markings as well as NO CLASSIFICATION marking.

4.3 Since the Policy was agreed, the Council has been progressing the best way of enforcing its use. This includes directions for staff on the use of the Policy and sourcing appropriate training.

4.4 An implementation plan for a phased system led solution to facilitate the classification of emails and documents was presented to the CMT in June 2015. This implementation was being led through the IGSG and included the procurement of classification software and guidance and training for staff.

4.5 Implementation of the email classification was dependent on the procurement process for the proposed software and the tie in with the upgrade to the email system.

## 5.0 IMPLEMENTATION

5.1 Whilst email classification software will enforce part of the Policy, the wider implementation will be in the form of raising its awareness amongst staff and includes training and guidance on how to classify information.

5.2 The email classification software is now deployed in ICT and they are working with the supplier to roll it out to the rest of the services by the end of September 2017 but hope to get this done sooner. User guidance will be issued to staff.

5.3 A Protective Marking, Sharing and Disclosing Information learning module has been developed and is being trialled through the Training and Development team. It will be available to all staff on the Council's e-learning platform Brightwave within the next month.

5.4 The Information Classification Policy (Appendix 1) has been reviewed to just explain what information classification is, and a separate Guide (Appendix 2) has been developed to provide staff with instructions on how to label, store, transmit and destroy information once a classification label has been determined.

5.5 Upon instruction from ICT when the software has been fully deployed, the Council's Information Governance Officer will send out a communication to inform all staff of the steps being taken to implement the Policy.

## 6.0 IMPLICATIONS

**Finance**

6.1 One off Costs

| Cost Centre | Budget Heading | Budget Years | Proposed Spend this Report £000 | Virement From | Other Comments |
|---|---|---|---|---|---|
| N/A | | | | | |

Annually Recurring Costs/ (Savings)

| Cost Centre | Budget Heading | With Effect from | Annual Net Impact £000 | Virement From (If Applicable) | Other Comments |
|---|---|---|---|---|---|
| N/A | | | | | |

**Legal**

6.2 The recommendations made in this report will ensure the Council's processes are in line with legislative requirements, including the Data Protection Act 1998, the Freedom of Information (Scotland) Act 2002, and the Public Records (Scotland) Act 2011.

**Human Resources**

6.3 The Information Classification Policy will place responsibilities on staff in conjunction with the Employee Code of Conduct in compliance with information governance, data protection and IT security responsibilities.

**Equalities**

6.4 None at this time, although recognition will be given to the wider and associate equalities agenda.

| | |
|---|---|
| | YES (see attached appendix) |
| √ | NO - This report does not introduce a new policy, function or strategy or recommend a change to an existing policy, function or strategy. Therefore, no Equality Impact Assessment is required. |

**Repopulation**

6.5 There are no direct repopulation implications arising from this report.

## 7.0 CONSULTATIONS

7.1 Consultation took place with the Council's Information Governance Steering Group.

## 8.0 BACKGROUND PAPERS

8.1 Information Classification Policy – Recommendation to implement a phased system led solution report to Committee, 22 September 2015.

**APPENDIX 1**

Inverclyde council

# *Information Governance and Management Framework*

# *Information Classification Policy*

Version 1.2

*Produced by:*
*Information Governance Steering Group*
*Inverclyde Council*
*Municipal Buildings*
*GREENOCK*
*PA15 1LX*

August 2015

**INVERCLYDE COUNCIL IS AN EQUAL OPPORTUNITIES EMPLOYER**
**THIS POLICY BOOKLET IS AVAILABLE ON REQUEST, IN LARGE PRINT, BRAILLE, ON AUDIOTAPE, OR COMPUTER DISC.**

## DOCUMENT CONTROL

| Document Responsibility | | |
|---|---|---|
| **Name** | **Title** | **Service** |
| Corporate Director, HSCP | Information Classification Policy | Information Governance and Management |
| | | |

| Change History | | |
|---|---|---|
| **Version** | **Date** | **Comments** |
| 1.0 | August 2013 | Draft Policy approved |
| 1.0 | April 2015 | Revised |
| 1.1 | August 2015 | Final Version |
| 1.2 | August 2017 | Revised to more simplified version to accommodate separate user guide. |
| | | |
| | | |
| | | |

| Distribution | | |
|---|---|---|
| **Name/ Title** | **Date** | **Comments** |
| | | |
| | | |
| | | |
| | | |

*Distribution may be made to others on request*

| Policy Review | | |
|---|---|---|
| **Review Date** | **Person Responsible** | **Service** |
| August 2019 | Information Governance Officer | Information Governance and Management |

| CLASSIFICATION | **OFFICIAL** |
|---|---|

## CONTENTS

## PURPOSE OF THIS POLICY

Information has varying degrees of sensitivity and criticality. Security classification of information is therefore required to ensure that the information processed within Inverclyde Council/HSCP receives the appropriate level of protection.

Every document generated has some value, and that value will depend on the views of the originator rather than the recipient, therefore the originator of a document must provide the classification and must agree or initiate any subsequent up or down grading.

Given this responsibility, many originators will opt for the safe choice and give all but the most innocuous documents the highest security classification. This practice leads to the debasement of the system. To reduce this risk a clear policy of document classification has been set up and all levels of staff made fully aware of the risks to the organisation, and to their future, of not applying the classification system intelligently.

The purpose of this Classification Policy is to provide the method of how to classify information and protect against the risk of unauthorised disclosure. This Policy should be read in conjunction with the Council's Information Classification: Policy Implementation Guide which provides examples of data types and classification as well as guidance on how to label, store, transmit and destroy information after it has been appropriately classified.

Unauthorised disclosure is the disclosure of information either accidentally or deliberately to (i) an individual including a family member, journalist or another employee who does not require access to the information or (ii) a facility i.e. the Internet or social media such as twitter or Facebook, with their being no authority in place for the viewing or disclosure of the information.

Information handled within a Classification Policy is shared/processed on a need to know basis and this Policy covers:

- The classification of information and appropriate marking or labelling to show the information has been classed as "Official". This should ensure the recipients know how to employ appropriate protection methods.
- The protection of information in an appropriate, practical and cost effective way that is proportionate

to the business risk of disclosure.

- The requirements of the Council's email system which has been configured to meet the UK Government's Secure Email Blueprint. This ensures that all emails sent by the Council/HSCP are secure by default.

**Who does this policy apply to?**

This policy applies to anyone with access to Inverclyde Council/HSCP data, records or information, including but not limited to employees, Councillors and 3rd party contractors.

**What does this policy not apply to?**

This policy does not apply to assessing whether information or data constitutes information which is exempt from disclosure by statute. This includes assessments made under the Freedom of Information (Scotland) Act 2002, the Environmental Information (Scotland) Regulations 2004, the Data Protection Act 1998 or the Local Government (Access to Information) Act 1985. Decisions on whether any statutory exemption is available will continue to be ultimately determined by the Head of Legal & Property Services.

Where it is determined that a statutory exemption is available and such exempt information is being transmitted, for example, internally by email, the email generated should be classified as Official or Official Sensitive and officers should follow the rules for handling and transmitting Official/Official Sensitive information contained within this Policy.

## 1 CLASSIFICATION SYSTEM

The following level is to be adopted and implemented throughout Inverclyde Council/HSCP.

Please note that it is for the originator to determine the correct protective marking. If this has not been done at the time the information was captured it should be done at the time the information is extracted, processed or otherwise handled. A "harm test" should be carried out to consider how sensitive the information is, the likely impact should the data be compromised or a deliberate or accidental unauthorised disclosure be made and whether the harm is hypothetical or more likely to occur than not.

Further guidance on classification including key questions is provided at Sections 3 and 5.

### OFFICIAL

This classification applies to the majority of information that is created or processed by the Council/HSCP. This includes routine business operations and services, some of which could have damaging consequences if lost, stolen or published in the media, but are not subject to a heightened risk profile.

This classification applies to information the disclosure of which could:

- Cause distress to individuals;
- Breach proper undertakings to maintain the confidence of third party information and intellectual property;
- Breach statutory restrictions on the disclosure of information;
- Cause financial loss or facilitate improper gain or advantage; or
- Disadvantage the Council/HSCP in policy or commercial negotiations with others.

Almost all information which is processed by the Council/HSCP lies within one Government classification of OFFICIAL. A sub-category with the OFFICIAL classification is OFFICIAL-SENSITIVE.

Information with the OFFICIAL classification must be labelled, numbered and accounted for with copies being distributed only to those with a specific need to know. It should never be copied without the originator's permission and must be kept in secure conditions.

All OFFICIAL documents must be controlled and destroyed in line with Inverclyde Council's Policy on the Retention and Disposal of Documents and Records. Computer files must also be protected by password controls.

In very limited circumstances, specific sensitivity considerations may warrant additional controls to reinforce the 'need to know' for access to certain information. Such information should be classed as OFFICIAL-SENSITIVE. This will apply to information previously referred to as "Private and Confidential" that is intended for the recipient only. OFFICIAL-SENSITIVE information requires elevated protection levels.

**OFFICIAL -SENSITIVE**

An OFFICIAL - SENSITIVE caveat should be applied where the 'need to know' must be most rigorously enforced, particularly where information may be being shared outside of a routine or well understood business process. For example, where the loss or compromise of information could have severely damaging consequences for an individual or group of individuals – there is a clear and justifiable requirement to reinforce the 'need to know principle' particularly rigorously across the organisation. The threshold for marking information OFFICIAL – SENSITIVE should be kept quite high. It is not intended that because an OFFICIAL document or data contains personal information it should be routinely marked OFFICIAL - SENSITIVE, it should meet the criteria set out in this paragraph.

As examples, this marking should be applied:

- to highly sensitive information that originates from the Lagan (CRM); the DWP CIS, Task FMS; Swift, SEEMIS and VISOR systems where disclosure could cause substantial distress to individuals;
- where it is mandated that the data can only be sent over a secure intranet connection (the Council's email system has been configured to meet the UK Government's Secure Email Blueprint. This ensures that all emails are secure by default).
- where disclosure could compromise or make it more difficult to maintain the operational effectiveness, internal stability or security of the Council/HSCP or undermine the proper management of the Council/HSCP;
- to personal sensitive information relating to an identifiable individual, which is sensitive information under the Data Protection Act[1]. Sensitive personal information under the DPA concerns:

a) the racial or ethnic origin of the individual,
b) his political opinions,
c) his religious beliefs,
d) whether he is a member of a trade union,
e) his health,
f) his sexual life,
g) the commission or alleged commission by him of any offence, or
h) any proceedings for any offence;

- to information formerly classified as "RESTRICTED" or "PRIVATE and CONFIDENTIAL" information;
- to highly confidential information;
- to commercially sensitive information; and
- to security information.

The Senior Information Risk Owner and Information Asset Owners need to make their own judgements about the value and sensitivity of the information that they manage, and decide the instances where it is appropriate to use the OFFICAL SENSITIVE caveat.

**NO CLASSIFICATION**

This applies to information that does not fall within an OFFICIAL or OFFICIAL SENSITIVE marking and is not subject to any specific marking or handling requirements. This information can be disclosed or disseminated without any restriction on content, audience and time of publication.

## 2 CLASSIFICATION LABELLING

Classification labelling applies to all forms of information both hard copy (paper) and electronic data including e-mail originated within Inverclyde Council/HSCP. All magnetic media, which includes floppy disks, CD ROMs, hard drives, removable hard drives etc. must be labelled commensurate with their contents.

Please refer to the Information Classification: Policy Implementation Guide for examples of data types and classification as well as guidance on how to label, store, transmit and destroy information after it has been classified.

## 3 DEGREE OF RISK

Classified information is protectively marked so that people know how to apply the appropriate security protection. The classification is dependent upon the impact or damage likely to occur if the information was leaked or disclosed to the wrong people.

The table below shows examples of the degree of risk afforded to the unauthorised disclosure of the above classification levels:

| Classification | Risk |
|---|---|
| **Official - Sensitive** | • Is applied to highly sensitive information from the Lagan CRM, the DWP CIS, Task FMS; Swift, SEEMIS and VISOR systems and all due care should be taken to protect this information by officers.<br><br>• Information whose unauthorised disclosure (even within Inverclyde Council/HSCP) would cause serious damage to the interests of the Council/HSCP. It would normally inflict harm by virtue of serious financial loss, severe loss of profitability or opportunity, grave embarrassment or loss of reputation. |
| **Official or Official - Sensitive caveat** | • When handling the personal data of individual(s). |
| **Official** | • For use on document/information that is contract or information that may harm the commercial interests of the Council/HSCP or a third party<br><br>• Should be used for draft policies etc. and other information that may harm the management of the Council/HSCP or 3rd parties should it be released |
| **No classification** | • These are documents generated and used daily for routine communication and require no special handling requirements. |

## 4 CHANGES IN CLASSIFICATION AND RETENTION OF DATA

Classification of data can change in relation to the circumstances in which the data was originated. An example might be classified budgetary information or information relating to redundancy information which may be Official-Sensitive during origination and formulation. Once this information has been released into the public domain it would require downgrading to No Classification.

The classification of data therefore requires regular review. Departmental managers shall implement local procedures to review the classification of data within their respective areas of control

Electronic and hardcopy data should not be retained longer than the periods recommended within Inverclyde Council's Policy for Retention and Disposal of Documents and Records.

## 5 CLASSIFICATION GUIDELINES

The classification of the data is the responsibility of the originator. The following guidelines are provided to assist the originator in deciding the appropriate classification level for the data. Classification of data is dependent upon:

- The degree of risk to Inverclyde Council/HSCP should the data be disclosed or passed to unauthorised personnel.
- The content of the data.
- The intended audience of the data.

The originator should ask the following questions before assigning a classification:

- Do I need to protect this information?
- How much protection is required?
- Is this information classified?
- Do I need to limit access to this information?
- What would happen if this data were disclosed to a third party?

Care must be taken not to over classify data. Work on the premise of who needs to know. For example when dealing with personal data ask the question, if this data were about me who should see it and how should it be protected? Any originator who has problems with the classification of data should consult their Line manager.

## 6 INFORMATION ASSET MANAGEMENT

An information asset is information that is valuable to the Council/HSCP's business, and will often be a collection of business files, for example the information held on the SWIFT social care system and any supporting files and documents would collectively be an information asset regardless of the format e.g. paper, electronic or microfilm. To assess whether something is an information asset consider whether:

- It has value to the Council/HSCP
- It would cost money to re-acquire
- There would be legal, reputational or financial repercussions if it could not be produced on request
- It would affect operational efficiency if it cannot be accessed easily
- There are risks associated with its loss, inaccuracy or inappropriate disclosure

Information Asset Owners are responsible for assigning a Classification to the assets they own, ensuring that the Classification category is recorded on the information asset inventory, and where possible ensure that the information produced or created from databases or using reporting software is protectively marked.

## 7 ANONYMISED AND NON PERSONAL DATA

Wherever practicable, or required, personal data will be anonymised before being shared. For example, the Council/HSCP may require to share employee information with potential bidders when re-tendering a service, to enable such bidders to assess any employee costs under the Transfer of Undertakings (TUPE) Regulations. Only anonymised employee information should be provided to such potential bidders. If required, officers should seek guidance from Legal Services on how to anonymise personal data before proceeding.

The specific rules which relate to the sharing of personal data do not automatically apply to anonymised and non-personal data. However, non-personal information may have conditions attached to its use. These can include any contractual restrictions or restrictions on re-use which may be imposed by the initial suppliers of such data. These include copyright or intellectual property rights or the indication of sensitivity or confidentiality, express or implied of the data which might mean that its release needs to be restricted. Where data has been supplied with a Protective Marking by another public sector body, the Council/HSCP is usually obliged to maintain that marking in any permitted re-use of the data.

The potential impact of these restrictions must be considered before deciding on the release of non-personal data. This should not be interpreted as a general way of blocking the release of otherwise unrestricted information.

## 8 WORKING WITH SECURITY CLASSIFICATIONS

When working with information assets, the following points need to be considered:

- Applying too high a marking can inhibit sharing and lead to unnecessary and expensive protective controls. This may mean that applying the handling/management restrictions could impede legitimate uses of the information;
- Applying too low a marking may result in inappropriate controls and potentially put sensitive assets at greater risk of compromise and lead to information not being adequately protected.
- The current information lifecycle (draft – finalised documents) – Information classification should be driven by an evaluation of the risk associated with unauthorised disclosure at each stage of a document's life cycle.
- Information contained within draft and/or early concept documents often has a higher degree of sensitivity, notably when there is a free and frank exchange of information, for the purposes of deliberation and decision making. Once a document has been finalised and is ready for distribution to its intended audience (perhaps by a committee or a management team following approval) the sensitivity of the information may have reduced, requiring a lower level of classification.
- Sensitive material published on intranet sites must also be clearly marked.
- Review the classification applied to similar documents/records that have been classified recently (within the last 12 – 18 months) – this can act as a good initial Guide.

Please refer to the Information Classification: Policy Implementation Guide for examples of data types and classification as well as guidance on how to label, store, transmit and destroy information after it has been classified.

## 9 PHOTOCOPYING AND PRINTING

Any employee having access to a photocopying machine can, in a matter of moments, copy any document to hand. Attention is drawn to the need to ensure confidentiality of all documents when they are copied.

When you print material, please ensure that it is collected immediately and that you collect all of the material. Secure printing should be used when printing classified documents.

## 10 UNIFIED CLASSIFICATION MARKINGS

Many organisations already have an information security programme in place that ensures consistent identification and protection of Official material. However assumptions cannot be made about how our trading partners may protect our information. Few organisations follow a common approach to sharing information securely. Exactly how information is classified and protected will vary from company to company, or even from department to department but steps should be taken so far as possible to ensure the level of protection is the same. For example, by contractually obliging our contractors, suppliers etc. to comply with this policy to the extent they are dealing with and/or generating Council/HSCP information.

In addition, adoption of this scheme by Inverclyde Partnership Organisations will provide current best practice guidance and interoperability on a common approach to appropriate marking and protection of information.

## 11 GOVERNANCE ARRANGEMENTS

### Responsibilities

Everyone is responsible for the information they handle. The Corporate Director (Chief Officer) Inverclyde HSCP has overall responsibility for updating this document and providing advice on its implementation.

### Other Relevant Policies / Council Documents

- Information Governance and Management Framework
- Acceptable Use of Information Systems Policy
- Policy for the Retention and Disposal of Documents and Records Paper and Electronic

- Records Management Policy
- Data Protection Policy
- A quick guide to Information Security
- Protocol for Dealing with a Potential Data Protection Breach
- Guidance on Promoting a Clear Desk Environment
- ICT Guide on Password Protection and Encryption
- USB Device Procedures

**Review Date**

This Information Classification Policy will be reviewed at regular intervals (initially after twelve months, and subsequently at least once every two years) and, if appropriate, it will then be amended to maintain its relevance. Further reviews will be instigated to reflect changes in legislation or standards.

**Compliance**

Random spot checks to review compliance with this Policy will be carried out as determined by the Corporate Director Inverclyde HSCP and by Internal Audit.

**Impact on the Council/HSCP's Key Priorities**

Without an up to date classification policy we risk unnecessary harm to people's personal data.

**Monitoring Arrangements**

All emails sent and received by the Council should be controlled and destroyed in line with Inverclyde Council's Policy on the Retention and Disposal of Documents and Records.

**Training and Awareness Requirements**

All users who have access to information that must be sent over the Council's email system will be trained in information security and protective marking, sharing and disclosing information before being allowed access to the system. This training will cover classification of documents.

**APPENDIX 2**

Inverclyde council

## *Information Governance and Management Framework*

# *Information Classification: Policy Implementation Guide*

Version 0.1

*Produced by:*
*Information Governance Steering Group*
*Inverclyde Council*
*Municipal Buildings*
*GREENOCK*
*PA15 1LX*

June 2017

disability confident EMPLOYER

**INVERCLYDE COUNCIL IS AN EQUAL OPPORTUNITIES EMPLOYER**
**THIS GUIDANCE BOOKLET IS AVAILABLE ON REQUEST, IN LARGE PRINT, BRAILLE, ON AUDIOTAPE, OR COMPUTER DISC.**

## DOCUMENT CONTROL

| Document Responsibility | | |
|---|---|---|
| **Name** | **Title** | **Service** |
| Corporate Director (Chief Officer) HSCP | Information Classification Policy Implementation Guide | Information Governance and Management |
| | | |

| Change History | | |
|---|---|---|
| **Version** | **Date** | **Comments** |
| 0.1 | | Draft |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |

| Distribution | | |
|---|---|---|
| **Name/ Title** | **Date** | **Comments** |
| | | |
| | | |
| | | |

*Distribution may be made to others on request*

| Policy Review | | |
|---|---|---|
| **Review Date** | **Person Responsible** | **Service** |
| 2019 | Information Governance Officer | Information Governance and Management |

| CLASSIFICATION | OFFICIAL |
|---|---|

## CONTENTS

## 1. Implementing the Information Classification Policy

This implementation guide must be read and used in conjunction with the Council's Information Classification Policy and the Acceptable Use of Information Systems Policy.

In general, the classification given to information and the associated protective marking label that is applied, is a shorthand way of signalling how information is to be handled and protected.

This guide:

- Provides guidance and tips on how to classify information accurately and consistently;
- Details when information should not be classified;
- Details how protective marking labels should be applied to physical and electronic documents;
- Details how information (in physical and electronic formats) is to be handled and managed depending on its classification i.e.
    - Storage and access
    - Transmission and
    - Destruction
- Advises where further help and advice is available.

## 2. The Council's Information Classification Scheme

The Council's information classification scheme has the following levels:

- **OFFICIAL**
- **OFFICIAL-SENSITIVE**
- **NO CLASSIFICATION**

All information which is processed by the Council/HSCP lies within one Government classification of OFFICIAL. A sub-category with the OFFICIAL classification is OFFICIAL-SENSITIVE. OFFICIAL-SENSITIVE information requires elevated protection levels. Please revert to the Council's Information

Classification Policy for further guidance on the Council's classification system.

In specific circumstances, descriptor can be used to identify certain categories of information that have already been assessed OFFICIAL-SENSITIVE. The descriptor should be applied in the format 'OFFICICAL-SENSITIVE (DESCRIPTOR)' *E.g. OFFICIAL SENSITIVE (PERSONNEL) / (FINANCE)*

Each level of classification indicates the level of protection that must be given to the information. The higher the level of protective marking, the more care must be taken when handling or managing the information.

## 3. Selecting an information classification

Please revert to the Council's Information Classification Policy for further guidance on the how to select the appropriate level of classification. APPENDIX A provides a definition of each information classification level and examples of documents/records that fall into each level.

### 3.1 **Classification**

- The creator of a document, record, or communication etc. should determine the initial classification level for that item and apply the protection marking label. Information Asset Owners are responsible for assigning a classification to the assets they own.

- APPENDIX A of this implementation guide provides direction on how to classify information. It is important to follow the direction provided in APPENDIX A as this will support consistent classification. Definitions of each classification level are provided (these mirror those provided in the Information Classification Policy). Examples of the range of documents, records etc. that would routinely fall within a classification level are also given.
    - If the information in question clearly falls within one of the classification levels as defined in APPENDIX A, then that level of classification must be applied.

- If you are unsure how to apply this Guide you should discuss the matter with your line manager, or seek advice – see Section **9 Contacts/further information.**

# 4. Applying protective marking

4.1 **General Points**

- Where an item is to be protectively marked, the label should be displayed prominently, so that the person using an item is clear as to the sensitivity of the information contained therein.
- The creator of the document **must** apply the protective marking label.
- To differentiate between the protective marking label and an incidental use of words, protective markings should always be displayed in UPPER CASE and where the formatting of the communication allows in **bold** typeface.

4.2 **Circumstances where no protective marking is required**

Where no protective marking requires to be given to information, for example, the information is public; the NO CLASSIFICATION label is to be applied.

4.3 **Protective marking labels**

These are:

- **OFFICIAL**
- **OFFICIAL-SENSITIVE**

4.4 **Applying protective marking to an electronic or physical document**

The protective marking should be clearly displayed on the top of each page of the document – normally as part of the document header.

4.4.1 **Formatting**

The label should be left justified, in UPPER CASE, font style bold, with a font size no less than 9 points.

4.5 **Applying protective marking to electronic documents where this is not possible to do so on each page**

Where possible this should be added to the metadata / item properties for a document. (i.e. in word; File; Info; you can select and add data for Properties – Related dates – Related people – Related

documents)

4.6 **Applying protective marking to a physical folder, document, binder, bankers box etc.**

The protective marking should reflect the marking for the **highest** level of protectively marked information contained within the folder etc.

4.6.1 **Formatting**

The label should be prominently displayed in UPPER CASE and font style bold. If the protective marking labels are hand written, pencil must not be used.

4.7 **Applying protective marking to an email**

The marking should be clearly displayed in the subject line of the email.

Users will be presented with the following:

| Classification: |
|---|

and will be required to choose a "classification" label from the drop down list before the email can be sent.

While Microsoft outlook has the functionality to add a security setting to email communications, if that facility is applied, the label that is generated may not be visible when the communication is read via a non-Microsoft email facility. It is important that the classification marking label is included in the subject line.

4.7.1 **Formatting**

The label should be the first element of the subject line, in UPPER CASE.

## 5. Changes to information classification over time

The sensitivity of some information can change over time, for example once information has been released into the public domain or when a document is no longer draft, where a final approved

version is available. There may be occasion when information should be re-assessed and where appropriate re-classify. As the costs associated with protecting information and the handling restrictions that accompany materials classified as OFFICIAL AND OFFICIAL-SENSITIVE are high Implementing unnecessary controls will result in expensive protective controls. The originator must agree or initiate any subsequent up or down grading.

Further information on Changes to information classification over time can be found in the Information Classification Policy.

## 6. Handling items according to their marking

APPENDIX B details how documents and records etc. should be:

- Stored including applying access restrictions;
- Transmitted i.e. disseminated; and
- Destroyed

As per the protective marking label assigned.

## 7. Roles and responsibilities for information classification and data storage

All staff who handle or use the Council's/HSCP's information, whether employed by the Council/HSCP or not, are personally accountable for following and implementing the rules and guidelines contained in this Guide and the Information Classification Policy. The information must be protected against all types of information security incidents. Individuals are personally responsible for protecting any information or other assets in their care.

Additionally, Council/HSCP management within directorates are responsible in their own areas for:

1) The security of information assets relating to their areas of business;
2) The assignment of appropriate classification labels to information, particularly when it is

appropriate to use the OFFICIAL-SENSITIVE classification;

3) The assignment of appropriate access restrictions to information, (it is the responsibility of the information asset owner to regulate access to information);
4) Governance, training and regulating staff including third parties who are granted access to information, (management must make sure that both staff who are employees and those who are not employees understand the basic security rules set out here);
5) Setting retention periods in that area as required by the Council's *Policy for the Retention and Disposal of Records Paper and Electronic;*
6) Ensuring information is destroyed in accordance with its classification label once the retention period has expired;
7) Compliance with the Council's legal and regulatory obligations; and
8) Determination of storage requirements and organisational management of the storage.

Technical responsibility for managing the Council's data storage lies with the infrastructure, service delivery within Information & Communication Technology (ICT).

## 8. Review

This implementation guide will be reviewed at regular intervals. The review period will be recorded on the accompanying coversheet. Any significant change to the Council's Information Classification Policy, the definition of personal and/or sensitive personal data, or Council policy or procedures primarily concerned with information governance may trigger an earlier review.

## 9. Contacts/further information

Enquiries regarding this implementation guide and/or the Information Classification Policy can in the first instance be directed to the Council's Information Governance Officer.

## 10. APPENDIX A

| INFORMATION CLASSIFICATION LEVEL | LEVEL DESCRIPTION | SERVICE | EXAMPLES |
|---|---|---|---|
| **OFFICIAL**<br><br>**'Available to all Council/HSCP staff'** | The majority of information that is created or processed by the Council/HSCP. Includes most policy development, service delivery, legal advice, personal data, contracts, statistics, case files and administrative data. | Finance Data | • Financial data relating to budgets and or corporate projects under review by Corporate Management Team. |
| | | ICT Information | • All passwords, combination settings and security keys |
| | | Legal documents | • Some Client information relating to litigation and/or proceedings.<br>•<br>• Names, addresses and dates of birth of Inverclyde Council/HSCP employees. |
| | | Organisational Development, Human Resources & Communications | • Incident reporting database/hard copy incident reports<br>o Injured party personal details<br>• Accident investigations<br>o Personal information of injured party<br>o Information on accident cause and concerns<br>o Information regarding claims<br>• Workplace assessments – personal details |
| | | Child/client data | • Names, addresses and dates of birth of Inverclyde Council/HSCP employees<br>• Children and Adults personal educational data. |
| | | Environment | • Lists of children on provision bus routes<br>• Some Planning Applications |
| | | Social Care | • Names, addresses and dates of birth of Inverclyde Council/HSCP employees |
| **OFFICIAL-SENSITIVE**<br><br>**'Accessed for business purposes only'** | This information is normally restricted to those staff who need access in order to carry out their duties. Such information is not made publicly available because | Any Department | • Open correspondence between Inverclyde Council/HSCP and others where disclosure would cause serious damage to the interests of the Council.<br>• Data relating to Confidential issue negotiations between firms tendering for contracts.<br>• Data relating to prices and contracts. |
| | | Financial Data | • Sundry Debtors Database (excel password protect). |

| INFORMATION CLASSIFICATION LEVEL | LEVEL DESCRIPTION | SERVICE | EXAMPLES |
|---|---|---|---|
| | of its sensitive nature e.g.<br>• Sensitive personal information<br>• Sensitive personnel information<br>• Commercial in confidence etc. | (Official-Sensitive may be used for these) | • Council Tax Payment Cards with name address and Council tax details (excel password protect).<br>• NDR database-non-domestic rates property details.<br>• Northgate – Council Tax information, properties and residents<br>• DWP CIS – Housing and Council Tax Benefit client and benefit information.<br>• Lagan CRM – Customer interaction with Inverclyde Council |
| | | Procurement (Official-Sensitive may be used for these) | • Electronic and hard copy tender returns. |
| | | Education | • SEEMIS Click and Go:<br>o Pupil personal information;<br>o Staff personal data;<br>o Pupil progress/end of term reports;<br>o SQA information<br>• SEEMIS ASN Records<br>• SEEMIS staff absence<br>• Email/hard copy Child Protection Data received from HSCP.<br>• SEEMIS/Hard copy children's files (children's centres) |
| | | Organisational Development, Human Resources & Communications (Official-Sensitive may be used for these) | • Pupil/service user risk assessments hard copy/electronic – Personal details and information.<br>• HR 21 – payroll records for employees<br>• SEEMIS – staff personal details and work undertaken<br>• Databases:<br>o Records of employee disciplinaries/grievances/sickness;<br>o Employee cases work details between HR staff, managers, employees, unions;<br>o Employee change of circumstances (e.g. bank details);<br>o Details of any draft confidential reports or proposals. |

| INFORMATION CLASSIFICATION LEVEL | LEVEL DESCRIPTION | SERVICE | EXAMPLES |
|---|---|---|---|
| | | Data sent by Government Secure Intranet | • Any information that is sent over government secure connection should be protected and restricted and this must be classified separately in the email subject.<br>• Restricted data is any data where it is mandated that the Council/HSCP must use a GSi account to transmit the data.<br>• Examples include MAPPA notifications. |
| | | Social Care | • Scottish Criminal Record Information:<br>o CHS Live (Criminal History Services); and<br>o SWIFT and hard copy<br>• VISOR (Violent and Sex Offenders Register).<br>• Older People in Care Homes database.<br><br>• Individual Client Records:<br>o CIS (Homecare); and<br>o SWIFT.<br><br>• Child Protection Minutes (Word)<br><br>• Children Excluded from School (Manual)<br><br>• ICIL (stock control system) – IJEMS (Access/SQL Server)<br><br>• Health Addictions of homeless clients contained on the Health and Homeless Information System Access Database.<br><br>• Questionnaire for LD clients contained in Access Database.<br><br>• Information contained on SWIFT for example:<br>o Foster Payments;<br>o Children in residential Homes; |

| INFORMATION CLASSIFICATION LEVEL | LEVEL DESCRIPTION | SERVICE | EXAMPLES |
|---|---|---|---|
| | | | o Adult Protection;<br>o Foster and Kinship Carers;<br>o Individual Client Records;<br>o Looked After Children's Register;<br>o Adoption and Fostering; and<br>o Foster Carer contact details.<br><br>The same classification should be applied where the above information is contained in anyone of the following:<br>• FMS, Excel, Access Database and Manual systems/formats. |
| **NO CLASSIFICATION**<br><br>**'available to all Council/HSCP staff and the general public'** | Can be published on the internet etc.<br>No restrictions on viewing (subject to publishing process required of publication scheme)<br>Declared records of interest. | Financial Data | • Normal financial data of a non-controversial nature, which could be in the public domain. |
| | | Procurement | • Advertisements of tender opportunities and advertised documents. |
| | | Legal documents | • Standard legal correspondence not relating to client details. |
| | | Organisational Development, Human Resources & Communications | • Standard day-to-day business meetings and minutes. |
| | | Child/client data | • Advertising e.g. clubs, services and voluntary groups |
| | | Environment | • Standard day to day administration |
| | | Social Care | • Standard day to day administration |

## 11. APPENDIX B

**Storage, transmission and destruction guidelines**

| **PHYSICAL INFORMATION** | | |
|---|---|---|
| **CLASSIFICTION LEVEL** | **STORAGE** | **DESTRUCTION** |
| **Official & Official-Sensitive** | <u>Secure Storage</u><br>• Locked filing cabinet/drawer within a locked room or building.<br>• Always physically secure when in transit e.g. locked briefcase.<br>• Appropriate third party storage. | <u>Irreversible destruction</u><br>• Cross-shredding<br>• Use of certified contractor |
| **ELECTRONIC INFORMATION** | | |
| **CLASSFICATION LEVEL** | **STORAGE** | **DESTRUCTION** |
| **Official & Official-Sensitive** | <u>Council network, EDMS or similar</u><br>• Store in appropriate file share, being mindful of the level of access to the share.<br><br><u>Portable storage devices (USB etc.)</u><br>• Only permitted where devices are, encrypted with Council approved software.<br>• Store in appropriate file share, being mindful of the level of access to the share.<br><br><u>Home working – using personally owned equipment</u><br>• No information to be held on devices that are not owned or under the control of the Council. | Council Policy on secure electronic destruction to be followed. |

**Transfer and dissemination advice:**

| Method of transfer | | Type of information | |
|---|---|---|---|
| | | **OFFICIAL** | **OFFICIAL-SENSITIVE** |
| Hand delivery | | ✓ | **NOTE 1** |
| Post or courier | Internal post | ✓ | **X** |
| | Standard external post | **NOTE 2** | **X** |
| | Registered post or dedicated courier from list of preferred couriers NOTE 8 | **NOTE 1, 2, 8** | **NOTE, 1, 2, 8** |

| Method of transfer | | Type of information | |
|---|---|---|---|
| | | **OFFICIAL** | **OFFICIAL-SENSITIVE** |
| Email | Internal e-mail | ✓ **NOTE 4** | **NOTE 1, 3, 4, 5, 6,** |
| | External e-mail | **NOTE 3, 4** | |
| Other electronic methods | Electronic file transfer | ✓ | **NOTE 1, 3, 4, 5, 6,** |
| | Telephone | **NOTE 7** | **If appropriate to transmit OFFICIAL – SENSTIVE data by telephone then see NOTE 7** |
| | Answering machines | **X** | **X** |
| | Fax transmission | **NOTE 9** | **NOTE 9** |

**NOTES**

1. The recipient should acknowledge receipt (signed, timed and dated) in writing, or provide a receipt electronically by automatic process.

2. There must be a named recipient, the envelope should be opaque and the classification should be not be marked on the outside of the envelope.
3. The subject line should begin with the classification in emails; the classification should be signified in other cases – for example in the file name.
4. This must not be used for sending information between Council/HSCP accounts and non-secure accounts.
5. There must be at least two layers of security for when; **a)** transferring it out of, or into, the corporate network electronically, or **b)** accessing the information on equipment that can be taken outside Council/HSCP premises.
6. Information must be password protected or encrypted and the password or encryption key must be sent by a separate route from the information that is being transferred.
7. Avoid being overheard in a public place and make the classification of the information discussion clear.
8. Couriers identity should be checked.
9. Fax should not be used as a means of transmission as these are no longer supported.