Inverclyde council

**AGENDA ITEM NO: 21**

| | | | |
|---|---|---|---|
| **Report To:** | **Policy and Resources Committee** | **Date:** | **22 September 2015** |
| **Report By:** | **Chief Officer, Inverclyde HSCP** | **Report No:** | **SW-16-2015-D** |
| **Contact Officer:** | **Dean Robinson Information Governance Officer** | **Contact No:** | **01475 712136** |
| **Subject:** | **Information Classification Policy - Recommendation to implement phased system led solution** | | |

## 1.0 PURPOSE

1.1 The purpose of this report is to present to the Committee implementation of the updated Classification Policy. The Council is recommending a phased system led solution to facilitate the classification of emails and documents.

## 2.0 SUMMARY

2.1 The Draft Classification Policy was agreed at the Policy and Resources Committee on 13 August 2013. It was agreed that a further report on the implementation of the Policy be submitted to Committee.

2.2 The Classification Policy presents a common approach to information classification and guidance for all services to use and assist them in establishing effective information classification practices.

2.3 There are several reasons why the classification of information is important including:

- Protection of personal and/or confidential information from unauthorised access or disclosure.
- Supporting routine disclosure and active dissemination of relevant information to the public.
- Facilitating information sharing with other services or external partners/agencies.
- Ensuring legal compliance in a number of areas including the Data Protection Act 1998, the Freedom of Information (Scotland) Act 2002 and the Public Records (Scotland) Act 2011.

2.4 The updates to the Policy reflect the changes to the UK Government Security Classifications. It has adopted a more simplified approach of having three levels of security classification: OFFICIAL, SECRET AND TOP SECRET. This marking is designed to be more robust and is suited to more modern workplaces and electronic information. The OFFICIAL marking will relate to the majority of information held by the Council. It will present significant changes to the Council in how emails and documents are transmitted electronically and labelled.

2.5 The updated Policy also introduces guidance on the transmission of personal and non-personal data, information exempt under statute, responsibilities for owners of critical information systems and the new suggested classification for different types of data.

2.6 As the majority of our information is transmitted electronically, the Council is recommending implementing software led solution to facilitate the classification of emails and word documents. This would simplify the process and ensure that all newly created documents are given a

classification.

## 3.0 RECOMMENDATIONS

3.1 That the Committee approve the updated Information Classification Policy (Appendix 1)

3.2 That the Committee note the finance details for the software to implement a phased system led approach for the classification and labelling of emails and word documents.

3.3 That a further report on the implementation of the Policy be submitted mid-2016.

**Brian Moore**
**Chief Officer, Inverclyde Director HSCP**

## 4.0 BACKGROUND

4.1 The Draft Information Classification Policy was agreed at the Policy and Resources Committee meeting on 13 August 2013.

4.2 The Council is committed to managing its information assets in a secure and appropriate manner and the Information Governance and Management Framework outlines the principles and practices for managing all information assets. Information classification is an important part of this framework.

4.3 The UK Government Security Classifications (GSC) policy requires that all UK government organisations classify their information assets into one of three types: OFFICIAL, SECRET and TOP SECRET. This simplified classification scheme replaces the previous Government Protective Marking Scheme (GPMS), making it easier for governing staff, contractors and service providers to safeguard government information.

4.4 All information used by Inverclyde Council is by definition **'OFFICIAL'**. It is highly unlikely the Council will work with 'SECRET' or 'TOP SECRET' information. Documents/records can be marked with a caveat: **'OFFICIAL-SENSITIVE'**. Information generated and used daily for routine communication and subject to Inverclyde Council's Policy on the Retention and Disposal of Documents and Records will require no special handling requirements and requires no classification marking.

4.5 Email continues to be the primary method for sharing information among employees, customers and partners. This presents a challenge for the Council that must protect information assets while promoting information sharing. The critical first step in solving this challenge is to classify email at the time of creation, so that the Council can identify the information's value, and manage the data accordingly.

4.6 Software for the system led classification ensures that all emails and word documents are classified and labelled before they can be saved, printed or sent via email.

4.7 The recommended software solution will help the Council comply with the new GSC policy by providing users with an easy way to classify their information assets. Users will be able to apply GSC compliant classifications and protective markings to email and documents to clearly identify information sensitivity. The software is configurable and will give us the option to define the classifications.

4.8 The software implementation for information classification will enable the Council to pilot the approach in a service area with a view to rolling this out further. The Council will be taking advice from the preferred vendor on the scale of the pilot and how it should be implemented.

## 5.0 PROPOSALS

5.1 Timescales will depend on the procurement process for the proposed system and will tie in with the proposed upgrade of the email system which is scheduled for completion January 2016. Implementation for the system led approach is proposed in March/April 2016. Appropriate training is being sourced to tie in with the implementation.

## 6.0 IMPLICATIONS

**Finance**

6.1 Implementation of a system led solution will have cost implications involving the purchase of software from the preferred vendor. Approval will be sought for this to be funded through the

Modernisation Fund.

Classification for Office complete with both Email and Document classification modules:

One off Costs (excluding VAT)

| Cost Centre | Budget Heading | Budget Years | Proposed Spend this Report £000 | Virement From | Other Comments |
|---|---|---|---|---|---|
| Modernisation Fund | | 2015/16 | 16 | | Funded from Modernisation EMR |

Annually Recurring Costs

CMT agreed that the on going costs should be funded on an equal share basis by the 3 Directorates.

| Cost Centre | Budget Heading | With Effect from | Annual Net Impact £000 | Virement From (If Applicable) | Other Comments |
|---|---|---|---|---|---|
| ICT | Maintenance | 2016/17 | 5 | Directorates | £1.7k to be vired from each Directorate to ICT |

6.2 Availability of awareness training will be sourced from the Clyde Valley Training Consortium who we work closely with. Any costs will be reported separately.

**Legal**

6.3 The phased system led approach will help to bring processes in line with regulatory and legislative requirements

**Human Resources**

6.4 The Policy itself does not have any personnel issues however, its implementation may have. Information Classification will place responsibilities on staff in compliance with information governance, data protection and IT security responsibilities.

**Equalities**

6.5 No equalities impact, although recognition will be given to the wider and associated equalities agenda.

**Repopulation**

6.6 There are no known repopulation implications.

## 7.0 CONSULTATIONS

7.1 Consultation took place with relevant officers who form part of the Information Governance Steering Group.

## 8.0 BACKGROUND PAPERS

8.1 Policy & Resources Committee Report 13 August 2013 – Draft Information Classification Policy.

***APPENDIX 1***

Inverclyde council

## *Information Governance and Management Framework*

# *Information Classification Policy*

Version 1.1

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

August 2015

## 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 |
| | | |
| | | |
| | | |
| | | |

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

*Distribution may be made to others on request*

| Policy Review | | |
|---|---|---|
| **Review Date** | **Person Responsible** | **Service** |
| | | |

Inverclyde council

**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 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, label, handle and transmit information and protect against the risk of unauthorised disclosure.

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.
- This policy incorporates the requirements of Government Connects within the classification policy, to

enable the Council to use the Government Secure Email Service.

**Who does this policy apply to?**

This policy applies to anyone with access to Inverclyde Council 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.

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 the likely impact should the data be compromised or an unauthorised disclosure be made.

Further guidance on classification including key questions is provided at Section 5.

## Official

This classification applies to the majority of information that is created or processed by the Council. 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 in policy or commercial negotiations with others.

Almost all personal information/data will be handled within Official without any caveat or descriptor. In very limited circumstances, specific sensitivity considerations may warrant additional controls to reinforce the 'need to know' for access to certain personal data at Official. This will apply to information referred to as "Private and Confidential" that is intended for the recipient only.

It 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.

There is no classification below the Official level. Therefore documents generated and used daily for routine communication and subject to Inverclyde Council's Policy on the Retention and Disposal of Documents and Records will have no labelling requirements and will require no specific additional handling requirements.

**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 above.

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 Government Secure Intranet connection.
- Where disclosure could make it more difficult to maintain the operational effectiveness of the Council or undermine the proper management of the Council.

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 Official-Sensitive caveat.

**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.

## 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. All magnetic media, which includes floppy disks, CD ROMs, hard drives, removable hard drives etc. must be labelled commensurate with their contents.

All hard copy data will be franked e.g. “OFFICIAL” or “OFFICIAL-SENSITIVE” caveat. Data processed electronically will bear the classification markings in the document header. Data containing personal, sensitive personal and business sensitive information must be transferred using the Government Connects system or encrypted to the current Council required level. If you are unsure always seek guidance from your Line Manager before sending this type of information.

## 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) would cause serious damage to the interests of the Council. 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 or a third party<br><br>• Should be used for draft policies etc. and other information that may harm the management of the Council or 3rd parties should it be released |
| **No classification marking required** | • 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 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 asks 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'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
- 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 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 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:

- There is no requirement to explicitly mark routine no classification assets.
- Applying too high a marking can inhibit sharing and lead to unnecessary and expensive protective controls;
- Applying too low a marking may result in inappropriate controls and potentially put sensitive assets at greater risk of compromise.
- When working with documents, classifications must be in CAPITALS at the top and bottom of each page. More sensitive information should be separated into appendices, so the main body can be distributed widely with fewer restrictions.
- Sensitive material published on intranet sites must also be clearly marked.
- It is good practice to reference the classification in the subject line and / or text of email communications. Where practicable systems should compel users to select a classification before sending, e.g. via a drop-down menu.

## 9 DATA TYPES AND CLASSIFICATION EXAMPLES

The table below (the list is not exhaustive) provides guidelines and examples of different types of data with a suggested classification. It should be noted that even if information is previously marked as Official it may still be releasable under the Freedom of Information (Scotland) Act 2002.

| Department | Classification | Data Content |
|---|---|---|
| | | |
| **Any** | **Official - Sensitive** | • Open correspondence between Inverclyde Council 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. |
| | | |
| **ICT Information** | **Official** | All passwords, Combination settings and Security Keys. |
| | | |
| **Finance Data** | **No classification** | Normal financial data of a non-controversial nature, which could be in the public domain. |
| | **Official** | Financial data relating to budgets and or corporate projects under review by Corporate Management Team. |
| | **Official – Sensitive caveat may be used** | Sundry Debtors Database (excel password protect).<br>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** | **No classification** | Advertisements of tender opportunities and advertised documents. |
| | **Official-Sensitive caveat may be** | • Electronic and hard copy tender |

| | | |
|---|---|---|
| | **used** | returns. |
| | | |
| **Education** | **Official-Sensitive caveat may be used** | • 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). |
| | | |
| **Legal documents** | **No Classification** | Standard legal correspondence not relating to client details. |
| | **Official** | • Client information relating to litigation and/or proceedings.<br>• Information obtained from Strathclyde Police in furtherance of litigation.<br>• Names, addresses and dates of birth of Inverclyde Council employees. |
| | | |
| **OD, HR & Comms** | **No Classification** | Standard day-to-day business meetings and minutes. |
| | **Official** | • Incident reporting Database/Hard copy incident reports:<br>o Injured Party personal details.<br>• Accident investigations electronic/hard copy:<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 |
| | **Official-Sensitive caveat may be used** | • Pupil/service user risk assessments hard copy/electronic – Personal details and information.<br>• Chris 21 – Payroll records for employees.<br>• SEEMIS – Staff personal details and work undertaken. |

| | | |
|---|---|---|
| | | • Databases:<br>Records of employee disciplinaries/grievances/sickness;<br>Employee case work details between HR staff, managers, employees, unions;<br>Employee change of circumstances (eg bank details);<br>Details of any draft confidential reports or proposals. |
| | | |
| **Child/client data** | **No classification** | Advertising e.g. Clubs, services and voluntary groups. |
| | **Official** | • Names, addresses and dates of birth of Inverclyde Council employees.<br>• Children and Adults personal educational data. |
| | | |
| **Environment** | **No Classification** | Standard day to day administration |
| | **Official** | • Lists of children on Provision Bus routes<br>• Some Planning Applications |
| | | |
| **GSi (Government Secure Intranet Information)/GCSX** | **Official-Sensitive caveat may be used** | • Any information that is sent over GSi should be protected or restricted and this must be classified appropriately in the email subject.<br>• Restricted data is any data where it is mandated that the Council must use a GSi account to transmit the data.<br>• Examples include MAPPA notifications. |
| | | |
| **Social Care** | **No classification** | Standard day to day administration |
| | **Official** | Names, addresses and dates of birth of Inverclyde Council employees. |
| | **Official-Sensitive caveat may be used** | • 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). |

| | | |
|---|---|---|
| | | • 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>• Foster Payments;<br>• Children in residential Homes;<br>• Adult Protection;<br>• Foster and Kinship Carers;<br>• Individual Client Records;<br>• Looked After Children's Register;<br>• Adoption and Fostering; and<br>• 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. |

## 10 CLASSIFICATION HANDLING CRITERIA

**The table below details the handling criteria for all Official Data:**

| Function | Classified Data |
|---|---|
| **User Access Limitations** | • Access limited to authorised data users on a need to know basis<br>• Access to ICT management systems is limited to authorised hierarchical constraints<br>• Standard password requirement<br>• Individual files may also be password protect at the discretion of the originator |
| **Transmission Restrictions E-Mail** | • Transmission from and to the Internet requires encryption<br>• Transmission across all areas of the Intranet and internally requires encryption |
| **Waste Disposal: Printed Format** | • Cross Cutting Shredded or Incinerated |
| **Waste Disposal: IT Media** | • Floppy disks and CDs destroyed by Shredding<br>• Hard Drives degaussed as arranged by ICT Services only<br>• Certificates must be raised confirming the cleansing of hard drives<br>• USB Devices must be handed to ICT Services for Secure Destruction, this will be completed by a security clear partner organisation |
| **Home Working** | • To be approved by the Operations Manager within the constraints of the Authority's Home Working Procedures |
| **Mobile Working** | • To be approved by the Operations Manager within the constraints of the Authority's Home Working Procedures |
| **Facsimile (Fax)** | • This method of transmission should only be used if there is no other method available.<br>• Authentication of reception before transmission is required.<br>• Confirmation of receipt is required.<br>• Pre-programmed telephone numbers entered to prevent miss dialling.<br>• Regular checks must take place to ensure that numbers have not changed. |

## 11 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.

## 12 PHYSICAL PROTECTION

**Any** document marked as Official should, without fail, be accounted for by signature and after the working day be locked away securely. A clear desk environment should be strictly enforced at all times.

## 13 SECURITY OF MEDIA IN TRANSIT

Envelopes containing Official documents should be clearly marked with the classification so that persons other than the intended level of recipient do not open it. If documents are to be carried by Public Carriers a second, outer envelope should be used showing destination address only and no indication of document classification. In addition the following procedures must be applied:

- Only reliable transport services should be used. A list of preferred couriers should be compiled and maintained within each service area. It is the head of service responsibility to maintain this list. Advice on how to pick appropriate secure suppliers can be provided by ICT Services.
- Procedures for checking a courier's identity should be implemented.
- Packaging of data should be sufficient to protect it from physical damage.
- A timed and dated sign off sheet evidencing delivery must be obtained

## 14 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 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.

## 15 GOVERNANCE ARRANGEMENTS

### Responsibilities

Everyone is responsible for the information they handle. The Corporate Director 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'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 go over the Government Secure Intranet (GCSX) will be trained in information security before being allowed access to the system. This training will cover classification of documents.