Inverclyde council

AGENDA ITEM NO: 13

Report To:	**Policy and Resources Committee**	**Date:**	**13 August 2013**
Report By:	**Corporate Director ICHCP**	**Report No:**	**CHCP/40/2013**
Contact Officer:	**Andi Priestman**	**Contact No:**	**01475 712251**
Subject:	**DRAFT INFORMATION CLASSIFICATION POLICY**		

1.0 PURPOSE

1.1 The purpose of this report is to present the draft Information Classification Policy for Members' approval.

2.0 SUMMARY

2.1 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.

2.2 This 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 The classification of information is also important for ensuring legal compliance in a number of areas including the Freedom of Information (Scotland) Act 2002 and the Data Protection Act 1998 and will support the Council in complying with the Public Records (Scotland) Act 2011.

2.4 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

2.5 The proposed categories of information classification have been developed to meet both organisational and operational needs based on the degree of risk of unauthorised disclosure and the impact or damage likely to occur. Due cognisance has been taken of the Government Protective Marking Scheme in developing these categories.

2.6 The policy sets out the categories which should be applied as follows:

- **Restricted** – information that is extremely sensitive and could cause substantial damage to the integrity, reputation or effective service delivery of the Council or significant distress to an individual.
- **Protect** – information that is sensitive to individuals or results in low levels of financial loss to individuals or third parties or disadvantages the Council in policy or commercial negotiations.
- **Unclassified** – Information that is created in the normal course of business that is unlikely to cause harm. Unclassified information includes information deemed public by legislation or through a policy of routine disclosure and active dissemination.

2.7 The Policy also sets out examples of practices in areas such as:

- Labelling information assets;
- Storing information;
- Transmitting information;
- Disposal of information no longer required;
- Allowing appropriate access and disclosure of information.

These practices are not intended to be prescriptive, rather they are identified within the policy as a guide and more detailed practices/protocols have been referred to later in the policy for employees to access.

2.8 Further work will be required to consider the most efficient and effective way to implement this policy and an action plan will be developed by the Working Group with a future report being submitted to CMT for approval.

3.0 RECOMMENDATIONS

3.1 It is recommended that Members:

a. Approve the Information Classification Policy
b. Agree that the Corporate Director, ICHCP, through the Information Governance and Management Working Group, brings a further report on the implementation of the Policy to Committee for approval.

Brian Moore
Corporate Director
ICHCP

4.0 BACKGROUND

4.1 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.

4.2 Information classification needs to balance the protection of information assets and the disclosure of information, as required by legislation, regulation and good business practice including Freedom of Information (Scotland) Act and the Data Protection Act 1998 and will support the Council in complying with the Public Records (Scotland) Act 2011.

4.4 Successful implementation of information classification will allow employees to perform their jobs effectively whilst preserving public confidence in the Council in the conduct of its affairs.

4.5 All employees who handle information need to be trained on information classification to understand why it is important, what it means and how to label and handle the information.

4.6 An effective programme for information classification will require ongoing monitoring and follow the established procedures for documenting and reporting any breaches of information security.

4.7 Since April 2013, the Council has piloted a number of Data Protection Act Training Workshops which covered the implementation of a data classification scheme for handling information.

5.0 IMPLICATIONS

5.1 Legal: The Information Classification Policy will bring processes in line with regulatory and legislative requirements where applicable.
Finance: There are no financial implications arising from this report.
Personnel: The Policy itself does not have any personnel issues however, its implementation may have. As stated above, following further investigation, this will be covered in a subsequent report to Committee.
Equalities: Due cognisance of equalities issues has been taken in the preparation of this report.

6.0 CONSULTATIONS

6.1 Extensive consultations took place with relevant Officers who form part of the Information Governance and Management Working Group as well as discussions with key officers within all Services to ensure a robust document is developed for the Council.

Inverclyde
council

INFORMATION

CLASSIFICATION POLICY

[Date of approval]

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 and the value of classification is fast becoming, by over use, commonplace. 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 organisations, and to their future, of not applying the classification system intelligently.

The purpose of this Classification Policy is to provide the method of how information is handled 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 is Confidential. 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 / procedure / protocol 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.

1. Classification System

Too many classes should be avoided and usually three levels are adequate. It is therefore proposed that the examples below are 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. When applying a protective marking please bear the following in mind:

- Applying too high a marking can inhibit access, lead to unnecessary expensive protective controls and impair the efficiency of the Council’s business; however

- Applying too low a protective marking may lead to damaging consequences for the Council and cause undue distress for the data subject(s) concerned.

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

Restricted

This applies to data the disclosure of which could:

- Cause substantial distress to individuals;
- Make it more difficult to maintain the operational effectiveness of the Council;
- Undermine the proper management of the Council;
- Cause financial loss or facilitate improper gain or advantage;
- Disadvantage the Council in policy or commercial negotiations with others;
- Breach proper undertakings to maintain the confidence of third party information; or
- Breach statutory restrictions on the disclosure of information.

For example, this marking should be applied to information that originates from the Lagan (CRM); the DWP CIS, Task FMS; Swift, SEEMIS and VISOR systems provided one or more of the above criteria apply to the information being considered. This marking should also be applied where it is mandated that the data can only be sent over a Government Secure Intranet connection.

Protect

This applies to information the disclosure of which could:

- Cause distress to individuals;
- Breach proper undertakings to maintain the confidence of third party information;
- 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.

A “PROTECT” marking is commonly applied to information referred to as “Private and Confidential”. It should therefore be applied to a document 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.

Both Restrict and Protect 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.

Unclassified

These are documents generated and used daily for routine communication and subject to Inverclyde Council’s Policy on the Retention and Disposal of Documents and Records, require no specific additional handling requirements.

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.

Restricted/Protect

All hard copy data will be franked top and bottom e.g. “RESTRICTED” or “PROTECT”. Data processed electronically will bear the classification markings in the document header and footer. Data with a restricted/protect classification 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 Potentially Restricted or Protect data.

Unclassified

This is data, which does not require marking.

3. .<u>Degree of Risk</u>

Classified information is protectively marked so that people know how to apply the appropriate security protection. The classification is dependant upon the impact or damage likely to occur if the information was leaked or disclosed to the wrong people. The table below shows the degree of risk afforded to the unauthorised disclosure of the above classification levels:

Classification	Risk
Restricted	Is applied to certain 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.
Protect	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.
Protect (Personal)	When handling one individuals personal data.
Protect (Private)	When handling more than one individuals personal data.
Protect (Commercial)	For use on document/information that is contract or information that may harm the commercial interests of the Council or a third party
Protect (Management)	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
Unclassified	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 would be Protect during origination and formulation. Once this information has been released into the public domain it would become unclassified and require downgrading.

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 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. 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 marked as Protect it may still be releasable under the Freedom of Information (Scotland) Act 2002.

Department	Classification	Data Content
Any	**Protect**	• Open correspondence between Inverclyde Council and others where disclosure would cause serious damage to the interests of the Council. • Data relating to Confidential issue negotiations between firms tendering for contracts. • Data relating to prices and contracts.
ICT Information	**Protect**	All passwords, Combination settings and Security Keys.
Finance Data	**Unclassified**	Normal financial data of a non-controversial nature, which could be in the public domain.
	Protect	Financial data relating to budgets and or corporate projects under review by Corporate Management Team.
	Restrict	Sundry Debtors Database (excel password protect). Council Tax Payment Cards with name address and Council tax details (excel password protect). NDR database-non-domestic rates property details. Northgate – Council Tax information, properties and residents. DWP CIS – Housing and Council Tax Benefit client and benefit information. Lagan CRM – Customer interaction with Inverclyde Council.
Procurement	**Unclassified**	Advertisements of tender opportunities and advertised documents.
	Restrict	• Electronic and hard copy tender returns.
Education	**Restrict**	• SEEMIS Click and Go: o Pupil personal information; o Staff personal data; o Pupil progress/end of term reports; o SQA information. • SEEMIS ASN Records. • SEEMIS staff absence.

		• Email/hard copy Child Protection Data received from CHCP. • SEEMIS/Hard copy children's files (children's centres).
Legal documents	**Unclassified**	Standard legal correspondence not relating to client details.
	Protect	• Client information relating to litigation and/or proceedings. • Information obtained from Strathclyde Police in furtherance of litigation. • Names, addresses and dates of birth of Inverclyde Council employees.
OD, HR & Comms	**Unclassified**	Standard day-to-day business meetings and minutes.
	Protect	• Incident reporting Database/Hard copy incident reports: o Injured Party personal details. • Accident investigations electronic/hard copy: o Personal Information of injured party; o Information on accident cause and concerns; o Information regarding claims. • Workplace assessments – personal details
	Restrict	• Pupil/service user risk assessments hard copy/electronic – Personal details and information. • Chris 21 – Payroll records for employees. • SEEMIS – Staff personal details and work undertaken. • Databases: Records of employee disciplinaries/grievances/sickness; Employee case work details between HR staff, managers, employees, unions; Employee change of circumstances (eg bank details); Details of any draft confidential reports or proposals.
Child/client data	**Unclassified**	Advertising e.g. Clubs, services and voluntary groups.
	Protect	• Names, addresses and dates of birth of Inverclyde Council employees. • Children and Adults personal educational data.

Environment	**Unclassified**	Standard day to day administration
	Protect	• Lists of children on Provision Bus routes • Some Planning Applications
GSi (Government Secure Intranet Information)/GSX	**Restrict**	• Any information that is sent over GSi should be protected or restricted and this must be classified appropriately in the email subject. • Restricted data is any data where it is mandated that the Council must use a GSi account to transmit the data. • Examples include MAPPA notifications.
Social Care	**Unclassified**	Standard day to day administration
	Protect	Names, addresses and dates of birth of Inverclyde Council employees.
	Restrict	• Scottish Criminal Record Information: o CHS Live (Criminal History Services); and o SWIFT and hard copy. • VISOR (Violent and Sex Offenders Register). • Older People in Care Homes database. • Individual Client Records: o CIS (Homecare); and o SWIFT. • Child Protection Minutes (Word). • Children Excluded from School (Manual). • ICIL (stock control system) – IJEMS (Access/SQL Server). • Health Addictions of homeless clients contained on the Health and Homeless Information System Access Database. • Questionnaire for LD clients contained in Access Database. • Information contained on SWIFT for example: • Foster Payments; • Children in residential Homes; • Adult Protection; • Foster and Kinship Carers; • Individual Client Records; • Looked After Children’s Register;

		• Adoption and Fostering; and • Foster Carer contact details. The same classification should be applied where the above information is contained in anyone of the following: • FMS, Excel, Access Database and Manual systems/formats.

7. Classification Handling Criteria

The table below details the handling criteria for all Protect Data:

Function	Classified Data
User Access Limitations	• Access limited to authorised data users on a need to know basis • Access to ICT management systems is limited to authorised hierarchical constraints • Standard password requirement • 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 • 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 • Hard Drives degaussed as arranged by ICT Services only • Certificates must be raised confirming the cleansing of hard drives • 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 Transitional Head of ICT within the constraints of the Authority’s Home Working Procedures
Mobile Working	To be approved by the Transitional Head of ICT within the constraints of the Authority’s Home Working Procedures
Facsimile (Fax)	• Authentication of reception before transmission is required. • Confirmation of receipt is required. • Pre-programmed telephone numbers entered to prevent miss dialling. • Regular checks must take place to ensure that numbers have not changed.

8. 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.

9. Physical Protection

The physical protection of Classified documents is comparatively simple. There are many fire proofed document containers available that offer good thief resistance. They range in size from dispatch box to full cupboard size and may be locked by either combination or keyed locks. Inbuilt alarm systems can be incorporated and these can be programmed to record all access to the documents.

Any Classified document should, without fail, be accounted for by signature and after the working day be secured as above. A clear desk policy should be strictly enforced at all times.

10. Security of Media in Transit

The physical protection of Classified documents in transit can be similarly protect and large offices should operate a messenger system with locked keys. The originator and the recipient hold the keys only.

Envelopes containing Classified 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.
- Special controls such as the use of locked containers, delivery by hand and tamper evident packaging should be used to further protect classified information from unauthorised disclosure.

11. Unified Classification Markings

Many organisations already have an information security programme in place that ensures consistent identification and protection of Classified 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 the level of protection should be the same.

Adoption of this scheme will provide current best practice guidance and interoperability on a common approach to appropriate marking and protection of information throughout Inverclyde Partnership Organisations.

12. Interoperability between Organisations

The table below defines the three security (IL) levels matched against the Government and Inverclyde Councils internal classification schemes. Individual Inverclyde Partnership Organisations should use their own terminology to describe these levels and should relate them to their business in terms of the impact or damage, which would arise from unauthorised disclosure. Information identified as IL2 or IL3 should always be marked whether it is on paper, cassette, disk, slide, flip chart, microfiche, photographs or any other media.

All Inverclyde Partnership Organisations can continue to use their own markings but should add the 'IL' marking at the end, to enable others to recognise the level of classification.

Government Department Classifications	Information Threat level	Inverclyde Council Document Classifications
Restricted	IL3	Restricted
Protect	IL2	Protect
Not Protectively Marked	IL1	Not Protectively Marked

Council Information should not be marked above Restricted.

Responsibilities

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

Other Relevant Policies / Council Documents

- Information Governance and Management Framework
- Classification Policy
- Acceptable Use of Information Systems Policy
- Guidance on Promoting a Clear Desk Environment
- Policy for the Retention and Disposal of Documents and Records
- Data Protection Policy
- A quick guide to Information Security
- Protocol for Dealing with a Potential Data Protection Breach
- ICT Guide on Password Protection and Encryption
- USB Device Procedures

Review Date

[ ]

Compliance

Random spot checks to review compliance with this Policy will be carried out as determined by the Corporate Director Inverclyde CHCP 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 (GSi) will be trained in information security before being allowed access to the system. This training will cover classification of documents.