Inverclyde council

AGENDA ITEM NO: 14

Report To:	**Policy and Resources Committee**	**Date:**	**3 June 2025**
Report By:	**Head of Legal, Democratic, Digital & Customer Services**	**Report No:**	**LS/033/25/VP**
Contact Officer:	**Vicky Pollock**	**Contact No:**	**01475 712180**
Subject:	**Information Classification Policy Update**		

1.0 PURPOSE AND SUMMARY

1.1 ☒ For Decision ☐For Information/Noting

1.2 The purpose of this report is to seek approval of an updated version of the Council's Information Classification Policy.

2.0 RECOMMENDATIONS

2.1 It is recommended that the Committee approves the updated Information Classification Policy appended to this report in Appendix 2.

Lynsey Brown
Head of Legal, Democratic, Digital & Customer Services

3.0 BACKGROUND AND CONTEXT

3.1 The Council is committed to managing its information assets in a secure and appropriate manner and the Council's suite of Information Governance policies and guidance outline the principles and practices for managing all information assets. Information classification is an important part of this information governance framework.

3.2 The Policy presents a common approach to information classification in line with national guidance and, together with the accompanying Information Classification: Policy Implementation Guide, provides direction to all services to use and assist them in establishing effective information classification practices.

3.3 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 and agencies.
- Ensuring legal compliance in a number of areas, including the Data Protection Act 2018, the UK General Data Protection Regulation, the Freedom of Information (Scotland) Act 2002 and the Public Records (Scotland) Act 2011.

3.4 Overall, the implementation of this Policy and associated systems across the Council is well established and has resulted in a more systematic and organised approach to information classification within the Council.

4.0 PROPOSALS

4.1 Review of the Council's Information Classification Policy

The Council's Information Classification Policy was last updated and approved in September 2017. The Policy has been reviewed and updated.

The policy remains fit for purpose and the classifications referred to in the policy still reflect national guidance. As such, only minor changes are recommended as a result of this review. The Policy has also been updated to reflect the Council's new policy template. A table which summarises the proposed changes to the Policy is set out at Appendix 1, with the revised Policy set out at Appendix 2 for Committee's consideration.

The operational Information Classification: Policy Implementation Guide has also been reviewed and updated and will be made available separately to staff and on ICON.

5.0 IMPLICATIONS

5.1 The table below shows whether risks and implications apply if the recommendation(s) is(are) agreed:

SUBJECT	YES	NO
Financial		X
Legal/Risk	X	
Human Resources	X	

Strategic (Partnership Plan/Council Plan)		X
Equalities, Fairer Scotland Duty & Children/Young People's Rights & Wellbeing		X
Environmental & Sustainability		X
Data Protection		X

5.2 **Finance**

One off Costs

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

Annually Recurring Costs/ (Savings)

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

5.3 **Legal/Risk**

The Council's Information Classification Policy assists the Council in ensuring compliance with regulatory and legislative requirements as set out in Paragraph 3.3 of this report.

5.4 **Human Resources**

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

5.5 **Strategic**

There are no strategic implications directly arising from this report.

5.6 **Equalities, Fairer Scotland Duty & Children/Young People**

(a) Equalities

This report has been considered under the Corporate Equalities Impact Assessment (EqIA) process with the following outcome:

	YES – Assessed as relevant, an EqIA is required and is available on the Council's website.
X	NO – This report does not introduce a new policy, function or strategy or recommend a substantive change to an existing policy, function or strategy. Therefore, assessed as not relevant and no EqIA is required. This Policy does not require an Equality Impact Assessment as there is no evidence to indicate that its contents could affect individuals differently or less favourably, on the grounds of their Protected Characteristics.

(b) Fairer Scotland Duty

If this report affects or proposes any major strategic decision:-

Has there been active consideration of how this report's recommendations reduce inequalities of outcome?

	YES – A written statement showing how this report's recommendations reduce inequalities of outcome caused by socio-economic disadvantage has been completed.
X	NO – Assessed as not relevant under the Fairer Scotland Duty for the following reasons: Provide reasons why the report has been assessed as not relevant.

(c) Children and Young People

Has a Children's Rights and Wellbeing Impact Assessment been carried out?

	YES – Assessed as relevant and a CRWIA is required.
X	NO – Assessed as not relevant as this report does not involve a new policy, function or strategy or recommends a substantive change to an existing policy, function or strategy which will have an impact on children's rights.

6.0 CONSULTATION

6.1 The Information Governance Steering Group and the Corporate Management Team have been consulted on the updated Information Classification Policy.

7.0 BACKGROUND PAPERS

7.1 None.

APPENDIX 1

SUMMARY OF PROPOSED REVISIONS TO INFORMATION CLASSIFICATION POLICY – APRIL 2025

PAGE	TITLE	SECTION	PROPOSED CHANGE
Throughout	n/a	n/a	Use of new policy template
5	Introduction and Purpose	3.1	Amendment to definition of Unauthorised Disclosure
6	Introduction and Purpose - What does this policy not apply to?	3.1.1	Updates to legislation
7	Classification System (Official)	3.2.1	Updated name of Retention and Disposal Policy
7	Classification System (Official-Sensitive)	3.2.2	Amended to replace specific systems with generic system types
8	Classification System(Official-Sensitive)	3.2.2	Update to definition of Special Category Data and Criminal Offence information
9	Degree of Risk	3.4	Amended to replace specific systems with generic system types
10	Changes in Classification and Retention of Data	3.5	Updated name of Retention and Disposal Policy
10	Information Asset Management	3.7	Amended to replace specific system with generic system type
13	Governance Arrangements – Responsibilities	3.12.1	Updated officer title
13	Governance Arrangements – Other Relevant Policies/Council Documents	3.12.2	Updated Policies/Council Documents

Appendix 2

Information Classification Policy

Version No 2.0

Produced by:

Information Governance Team
Inverclyde Council
Municipal Buildings
GREENOCK
PA15 1LX

Inverclyde Council is an Equal Opportunities employer.

This document can be made available in other languages, large print, and audio format upon request.

Document Control

Document Responsibility		
Policy Title	**Corporate Group**	**Service**
Information Classification Policy	Information Governance Steering Group	Legal, Democratic, Digital & Customer Services

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
2.0	April 2025	Updated to new policy format, review and update of policy.

Distribution
Corporate Directors, Heads of Service, ICON, Information Governance Steering Group

Policy Review		
Updating Frequency	**Next Review Date**	**Responsible Officer**
3 years	June 2028	Head of Legal, Democratic, Digital & Customer Services

Policy Review and Approval			
Name	**Action**	**Date**	**Communication**
Policy & Resources Committee			ICON; IGSG;

CONTENTS

1 INTRODUCTION

1.1 Executive Summary

Inverclyde Council is committed to managing its information assets in a secure and appropriate manner. This Policy sets out the basis by which information will be classified to make sure its sensitivity, integrity and availability is maintained throughout its life, particularly in terms of when it is communicated or transmitted. All information must be classified and marked to show how sensitive it is. This classified marking then decides what level of protection must be applied to the information.

1.2 Background

This Policy and the associated Policy Implementation Guide presents a common approach to information classification and guidance for all services to use and assist them in establishing effective classification practices.

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 2018, the UK General Data Protection Regulation, the Freedom of Information (Scotland) Act 2002 and the Public Records (Scotland) Act 2011.

1.3 Strategic Context

There are no strategic implications arising from this Policy.

1.4 Links to Legislation

This Policy considers relevant legislation and regulatory requirements including the Public Records (Scotland) Act 2011, the Freedom of Information (Scotland) Act 2002, the Data Protection Act 2018 and the UK General Data Protection Regulation.

1.5 Links to Corporate Groups

This Policy is linked to the work of the Information Governance Steering Group.

2 SCOPE

This Policy applies to all information assets (including both paper and electronic documents) created or used within Inverclyde Council, but it is especially relevant and important for employees who deal with sensitive information concerning members of the public, employees or Council services.

3 POLICY CONTENT

3.1 Introduction and Purpose

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 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 refers to the disclosure of information to individuals (e.g. a family member, journalist or another employee), entities (e.g. an outside company) or systems (e.g. a social media platform) that are not permitted to receive it. This can either be accidental or deliberate.

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.

3.1.1 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 legislation. This includes assessments made under the Freedom of Information (Scotland) Act 2002, the Environmental Information (Scotland) Regulations 2004, the Data Protection Act 2018, the UK General Data Protection Regulation or the Local Government (Access to Information) Act 1985.

Where it is determined that an 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.

3.2 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 3.4 and 3.6.

3.2.1 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 Records Retention and Disposal Policy. 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.

3.2.2 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 Customer Management, UK and Scottish Government Social Security, Finance Management, Social Care and Social Work Case Management, Education Management & Information 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 and special category information as defined by data protection law relating to an identifiable individual. Special category information consists of:
  a) racial or ethnic origin
  b) political opinions
  c) religious or philosophical beliefs
  d) trade union membership
  e) health information
  f) sex life or sexual orientation
  g) genetic information
  h) biometric information (where used for identification purposes)
- to information relating to criminal convictions or proceedings and criminal outcomes and sentences
- to information relating to offences (including alleged offences)
- 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.

3.2.3 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.

3.3 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.

3.4 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 Customer Management, UK and Scottish Government Social Security, Finance Management, Social Care and Social Work Case Management, Education Management & Information and VISOR systems and all due care should be taken to protect this information by officers. • 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 contractual or information that may harm the commercial interests of the Council/HSCP or a third party • Should be used for draft policies etc. and other information that may harm the management of the Council/HSCP or third parties should it be released
No classification	• These are documents generated and used daily for routine communication and require no special handling requirements.

3.5 Changes in Classification and Retention of Data

Classification of data can change in relation to the circumstances in which the data 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 Records Retention and Disposal Policy.

3.6 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.

3.7 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 Social Care and Social Work Case management 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 Register, and where possible ensure that the information produced or created from databases or using reporting software is protectively marked.

3.8 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.

3.9 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.

3.10 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.

3.11 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.

3.12 Governance Arrangements

3.12.1 Responsibilities

Everyone is responsible for the information they handle. The Head of Legal, Democratic Digital and Customer Services has overall responsibility for updating this document and providing advice on its implementation.

3.12.2 Other Relevant Policies/Council Documents

- Information Governance and Management Framework
- Acceptable Use of Information Systems Policy
- Records Retention and Disposal Policy
- Records Management Policy
- Data Protection Policy
- A quick guide to Information Security
- Data Breach Management Protocol
- Clear Desk Guidelines
- Information Sharing Protocol
- ICT Guide on Password Protection and Encryption
- USB Device Procedures

3.12.3 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.

4 ROLES AND RESPONSIBILITIES

This policy applies to everyone who handles, or processes, Inverclyde Council/HSCP information, including, but not limited to, employees, Elected Members and third party contractors.

5 IMPLEMENTATION

5.1 Communication of the Policy

This Policy, along with the associated Policy Implementation Guide, will be available on ICON (the Council intranet).

6 RISK

6.1 Legislative Risk

This Policy takes into account various legislative requirements, including the Public Records (Scotland) Act 2011, the Freedom of Information (Scotland) Act 2022, the Data Protection Act 2018 and the UK General Data Protection Regulation.

For the avoidance of doubt and in the event of a conflict between legislation, policy or best practice guidelines, legislation must take priority. This also applies to any future legislation which may be enacted.

7 EQUALITIES

7.1 Consultation and Engagement

This Policy was updated in consultation with the Corporate Management Team and the Information Governance Steering Group.

7.2 Equality Impact Assessment

This Policy does not require an Equality Impact Assessment as there is no evidence to indicate that its contents could affect individuals differently or less favourably, on the grounds of their Protected Characteristics.