Information Security Classification Procedure

1. Introduction

1.1 The Council's the Information Management and Handling Policy states that information must be classified. Information which is Personal or has an element of operational sensitivity must be marked with a classification label to identify that it requires careful handling in order to meet legal or contractual obligations. When this threshold is defined, information is allocated the classification label of **PROTECT**.

2. Legislation, Codes of Practice and Standards

2.1 In the event of an apparent conflict of handling or security instruction occurring between

a. Council Policy, Sharing Agreements or Professional Codes of Practice, staff must apply whichever instruction meets the higher security standard.

b. Legislation, Legislation must take priority.

2.2 In the event of an apparent conflict occurring, staff should bring the matter to the attention of the Information Security Officer (ISO) through their line manager, so council procedures can be reviewed and amended if required.

3. Roles and Responsibilities

3.1 Managers must:

a. Identify what information used within their Department is to be marked as **PROTECT** or if there is a requirement to increase to the **PROTECT+** level.

b. Take appropriate steps to ensure staff are made aware of what information is designated as **PROTECT** and provide staff with training and awareness of the working practices to be followed. This must also be communicated to non ERC individuals and third party organisations such as agency staff, consultants, work experience students, volunteers or organisations processing or storing Council information on the Council's behalf eg., providing a support service using client information provided by the Council or where the Council stores information on a server owned by another organisation. The preferred method of communication is via the ERC Information Security Sharing Agreement.

c. Provide regular reminders to staff of the handling instructions (at least once a year) and more frequently (at least twice a year) where **PROTECT+** is applied

d. Be able to provide evidence of who has and has not been informed of information security and data protection policies and received training in both.

e. Ensure staff are supplied with the right equipment to meet the chosen handling instructions (for example providing sturdy briefcases, document wallets or portfolios to safely carry paperwork).

3.2 Staff must:

a. Ensure they are aware of and apply the instructions allocated to information they handle.

b. Alert their line manager if they believe an instruction is not adequate; where equipment provided is inadequate or where instructions conflict with those from other sources such as Sharing Agreements, Contracts or professional Codes of Practice.

c. Clearly mark documents and emails as **PROTECT** where necessary (using capital letters and bold text)

4. How to use the scheme

4.1 No marking indicates the information is below the threshold for **PROTECT** therefore normal duty of care practices are sufficient when handling that information.

4.2 **PROTECT** marking indicates protective action is necessary and applies to:

- PERSONAL information, as defined by the Data Protection Act, where a name or other identifying factor is documented along with other details such as address, phone number, details of services being provided or medical conditions (Note, this could include Attendance Registers).
- OPERATIONAL information where there is an expectation of a 'need to know' for example, details of security practices or of how the Council reacts to a civil emergency or details of Council budgets or tenders which are pending approval.

4.3 **PROTECT+** indicates that additional protective measures are necessary because there is a higher than average degree of sensitivity. This will only be used for information that falls under the Data Protection Act's definition of Personal Sensitive (See 4.6). Examples of where this might apply include application forms that capture a full life history such as benefit applications, sex offender or criminal history details or about children or vulnerable persons. It may also be applied to some operational instructions such as those that give detailed information about how the Council would react to a civil emergency.

4.4 Most Public Sector agencies classify information labels and these map to the ERC label as follows:

Common Labels	ERC Label
Impact Level 0, Unclassified, None, Green, Public, Not Protectively Marked	None
Impact Level 1, Unclassified, None, Green, Internal, Private, Not Protectively Marked	None
Impact Level 2, Personal, Internal, Protect, Amber, Private or Private & Confidential	**PROTECT**
Impact Level 3, Personal, Protect, Restricted, Eyes Only, Personal & Confidential, To be Opened by Addressee only, Amber	**PROTECT**
Impact Level 4, Confidential, Red, Eyes Only	**PROTECT+**

4.5 Additional Markings

Information may also have additional markings. These can include limits on distribution such as 'Addressee Only' or 'Members Only', 'Private and Confidential' or relate to the nature of content. Use of these additional markings is at the discretion of the Department but if used, Departments must:

- document the terms that may be used
- define why and when they can be used
- make the instructions easily available to staff to refer to
- ensure staff understand that that there is a difference between the two as it is the classification label that takes precedence so the two must be used together.

4.6 Personal and Personal Sensitive Definitions

Information relating to a living individual is Personal or Personal Sensitive information and falls under the Data Protection Act. Be wary though, a name is not the only way to identify a person so exclusion of the name does not automatically mean it is not Personal. A post code tied with a rare medical condition could single out an individual for example. At a very high and generic level, the following table is a definition of how the Data Protection Act identifies Personal vs Personal Sensitive details. If you are still not sure then seek advice from the ISO or Legal Department.

Personal	• **Personal** (names, addresses, contact details, age, sex, birth details, physical descriptions, NI number) • **Family** (marriage, partnership or marital history, details of family & other household members, habits, hosing, travel details, leisure activities, membership of charitable or voluntary organisations) • **Employment** (employment & career history, recruitment & termination details, attendance record, health and safety records, performance appraisals, training records, security records, payroll or User ID) • **Financial** (income, salary, assets and investments, payments, credit worthiness, loans, benefits, grants, insurance details, pension info) • **Goods or services** (goods or services supplied to a person, licences issued, agreements and contracts • **Expressions & Opinions** - any expression of opinion about an individual and any indication of the intentions of the data controller or any other person in respect of the individual
Personal Sensitive	• Racial or ethnic origin • Political opinions • Religious or other beliefs of similar nature • Trade union membership • Physical or mental health • Sexual life • Criminal convictions or proceedings • Criminal outcome & sentences • Offences (including alleged offences)

4.7 Marking Documents

4.7.1 When documents are generated which contain **PROTECT** information, they must be marked. This does not apply to documents or emails that are generated externally for example, a letter sent by a customer or a Doctor.

4.7.2 ERC does not currently have an automated method for marking the word **PROTECT** to a document or email, so staff will need to mark documents manually as follows:

a. Word or Excel documents - add **PROTECT** to the header and footer of each page.

b. Email - add **PROTECT** to the subject header. If responding to an email that is classified by the originator, then only add your own classification statement if you have added information to the reply that requires **PROTECT** to be used.

c. Paper - either stamp or handwrite the classification level at the top and bottom of each page. As few staff create a handwritten document, it is not anticipated that this method would be needed often.

d. Databases – databases are often used to generate bulk communications for example, Carefirst, Lagan or Council Tax. Information printed from these databases will only be marked where the system itself is capable of labelling it. If the database has the functionality but does not use the term **PROTECT**, contact the ISO to discuss the most appropriate alternative option.

e. Additional Markings - Letters to customers and other agencies should only be marked with additional markings where it is already common practice to use one for example HR often use the label 'Personal' or 'Private' or social workers notifying a client of support treatment might mark it as 'Personal & Confidential'. These are not to be used in isolation, the **PROTECT** classification must also be applied.

f. Other – It may not be possible to directly mark some forms of information but alternatives should be considered for example, photographs (mark on the back), video (mark on the casing), voice recordings (state what it is at the start of the recording) or backup tapes (mark on the casing).

4.8 Exceptions

4.8.1 Where a manager believes that their staff face exceptional circumstances which mean they will be unable to fully comply with handling instructions, they must first raise the matter with a Senior Manager and discuss what alternative options exist bearing in mind that just because something which has always been done in a particular way does not meant that it is still relevant today. If the Manager agrees there is no alternative, then they must submit a request for an exception to the ISO.

4.8.2 Managers are strongly advised to review working practices first, in order to determine if staff could change working practices to remove the need for an exception in the first place.

4.8.3 If the ISO approves the request, additional protective measures may be required. Departments must ensure that these are implemented locally as indicated.

5. Further Information

5.1 For more information about information classification or mapping to a scheme used by another agency, contact Carol Peters, Information Security Officer on 0141 577 8649.