

1. Introduction

At its simplest, protective marking (or classification as it is sometimes referred to) is a way of assigning information to a security label which in turn, relates to a range of pre-defined controls designed to ensure the information is handled properly by all parties.

Documenting guidelines is important as, without something for people to refer to, the decision on what is or is not 'adequate' protection is left up to the individual. This leads to a wide range of practices; from the very inadequate to over protection.

This disparity is a significant risk to any organisation as the Data Protection Act requires that data is consistently handled and secured appropriately, especially when sharing with other parties.

2. Data Protection and Freedom of Information

Customer First is a data processor on behalf of the 32 local authorities, who are the data custodians. These guidelines have been written to tie in with local authority security standards as far as is possible and to offer assurances of the minimum security controls that the SNI will afford to information and in particular, Personal information.

Protective Marking is not designed to interfere with the Freedom of Information (Scotland) Act (FOISA) in terms of public bodies being open and transparent. However, occasionally, it is inappropriate to release information under FOISA. The Act makes allowances to consider exempting release of information where doing so would result in 'real and significant damage to the authority or other people' or where the information is personal (a breach of the Data Protection Act). As such, Protective Marking Schemes should work alongside FOISA Publication Schemes by offering guidance on safe and secure handling of personal or other information which requires careful consideration on whether or not to release it, something which the Publication Scheme itself is not designed to do.

However, even if information is covered by the Protective Marking Scheme and not the FOISA Publication Scheme that does not mean that it should not be released on receipt of a request. Departments must still consider in full any requests received and take appropriate legal advice. There is no black and white answer and each case must be treated on its own merits. The main thing to bear in mind is that no matter what classification is allocated, that does not give permission automatically to refuse release.

3. Protective Marking Scheme

Controls are incremental so you must ensure that you have applied all the controls listed in lower categories as well as those in the chosen category. SNI approved guidelines are listed. Alternatives will be considered but must be approved by the SNI Support Office.

A few examples are listed, but you shouldn't consider that to mean that these are definitive. Sometimes content differs and could mean a document should be treated with more consideration than its normal counterparts e.g. CAS Personal Record is very basic, almost public domain information so is Protect but only on the basis that it is personal information. NPLD Personal Records however contain indicators around health and criminal convictions which are much more sensitive therefore those Personal Records would be Confidential.

The Impact Level (IL) allocated to each classification relates to the HMG Protective Marking Scheme but should not be considered definitive. The main reason it is there is to allow Information Security professionals to consider implications across the two standards.

The controls apply to the SNI Support Office or its agents such as Lead Authorities who are designated a role in the management, support and maintenance of the SNI and its business systems. Local Authorities, as Data Custodians, must refer to their own local guidelines.

Information which originates from outwith the SNI may not be protectively marked when received or may have its own protective marking level. If not protectively marked already, then mark it in line with this Guideline.

If it was protectively marked by the originator, then you should have been issued with instructions on how to handle it. These should be respected and the information handled accordingly. If the handling instructions are lower than those that the SNI would normally apply to the same information internally, then apply our higher level of controls anyway.

If no handling instructions were issued, ask the originator for instructions or identify what protective marking the SNI would afford and handle it accordingly.

Some organisations also use 'Descriptors' which provide an indication of why documents are marked in the manner that they have been. Descriptors are not used within the SNI. However as it is possible that staff may receive information from someone who does, a brief explanation has been included.

Descriptors are usually recorded next to the protective marking (for example PROTECT PERSONAL), with the most common being:

- Personal – Information that contains personal information of an individual
- Commercial – information, the release of which may, would, or be likely to, prejudice the commercial interests of the Council or a third party
- Policy/Strategy – information that forms part of a council policy or strategy or procedure that is normally associated with internal use only
- Investigation – information that may prejudice a criminal investigation, prosecution or apprehension of an offender
- In Confidence – information received under an air of confidence, the disclosure of which would be an actionable breach in law

4. Roles And Responsibilities

Originators the person creating a document (or any other format of information) is responsible for setting the Protective Marking of that particular document/information (digital or paper) when they create it. Over time it might be necessary to change the protective marking of information; this is also a responsibility of the originator.

Line managers are responsible for ensuring that marking of sensitive information is done in accordance with the guidance provided. They have to keep in mind the availability of information for others and the impact involved with high protective marking.

Users can challenge the applied protective marking. They can never change the marking: that has to be applied by the originator of the information or a successor (if the originator can not be traced). All employees in possession of information (or copies of the information in a form of carrier) with a protective marking are responsible for handling the information in accordance with this marking. This includes storing, processing, sharing and destroying in accordance with this policy.

Information Security Officer provides advice on the protective marking of information.

For specific advice or just general guidance, contact the Information Security Officer via the SNI Support Office.

5. Protective Marking Scheme

Identify the worst impact of a compromise to identify the marking level then check the table for guidance on how to handle it in different situations.

CATEGORY	NONE (IL0)	PROTECT (IL1-2)	RESTRICTED (IL3)	CONFIDENTIAL (IL4)
Examples	<ul style="list-style-type: none"> All documents listed in the FoISA Publication Scheme Official communications or council publications, except where these contain details of activity such as security measures, network or system application components or how operational support is provided. Policy documents which do not give details of security measures Professional Personal details such as name, job title, work phone number or work email 	<ul style="list-style-type: none"> A single CAS Personal Record Record or information about a single citizen which would be subject to the Data Protection Act Personally identifiable records such as Personnel Files, Customer records, staff health records, staff pay records General information relating to service delivery which if compromised or damaged, may cause inconvenience citizens Financial records 	<ul style="list-style-type: none"> A single NPLD Personal Record unless other IL4 criteria are met Aggregations of <100 CAS Personal Records Minutes of meetings, project reports, bids prior to award, contracts during negotiation NHS Health records Risk or vulnerability assessments. Privacy impact reports, security documents, network schematics, network and physical security measures used to combat threats 	<ul style="list-style-type: none"> >100 CAS Personal Records Aggregations of NPLD Personal Records Network diagrams, system build instructions, procedures or guidelines which discuss details of IT security standards or systems such as intrusion detection auditing, monitoring etc Policies or procedures relating to police matters or sensitive health records, including Witness or Child Protection or other individual protective measures
Impact of compromise	<ul style="list-style-type: none"> No affect to service delivery to the customer or general operations No danger, discomfort or embarrassment to individuals No breach of statutory obligations 	<ul style="list-style-type: none"> Minor breach of statutory obligations or duty of confidence Cause discomfort or embarrassment to an individual Reduce an individual citizen's perception of a service (e.g. a compromise leading to the cancellation of a hospital appointment) Cause loss to the Public or Private sector of up to £1000 or £100 for an individual or sole trader. 	<ul style="list-style-type: none"> Clear breach of statutory obligations Prolonged distress or danger to an individual or risk to personal safety Cause danger, discomfort or embarrassment to many citizens Disruption to service delivery, operations or disadvantage a local authority release may undermine citizen confidence in the SNI Cause loss to the Public or Private sector of up to £10,000 or £1,000 for an individual or sole trader 	<ul style="list-style-type: none"> Significant breach of statutory obligations Significant political harm or disadvantage to local or national government Significant disruption to operations or service delivery or flawed working services which could pose an increased risk to health and safety Cause a loss to the Public or Private sector of over £10,000 or £1,000 for an individual or sole trader
Disclosure to other parties	<ul style="list-style-type: none"> Freely available without restriction. 	<ul style="list-style-type: none"> Confirm legitimate entitlement exists to share personal data & seek DPA & Information Security advice. Risk assess the exchange methods & use by 3rd parties (A Privacy Impact Assessment may be needed for personal data) Information Sharing Protocol required between all parties SNI Support Office authority required. 		

Scottish National Infrastructure
Guideline for Protectively Marking Information

CATEGORY	NONE (IL0)	PROTECT (IL1-2)	RESTRICTED (IL3)	CONFIDENTIAL (IL4)
		<ul style="list-style-type: none"> Maintain a record of the exchange. 		
Post (and internal mail system)	<ul style="list-style-type: none"> Use due diligence to protect against accidental compromise 	<ul style="list-style-type: none"> Single personal mail can be posted normally, addressed to a named individual and ideally marked as Private. Bulk records must not be sent in the post, instead use electronic methods for transfer. 	<ul style="list-style-type: none"> Clearly mark for the attention of a named recipient. 	<ul style="list-style-type: none"> Use new, fully sealed envelopes Hand deliver or use trusted (bonded) courier that requires signature on pickup and receipt and tracks the delivery. Double envelope with only internal envelope being marked as 'Private & Confidential for external mail of single records. Consider using tamper proof measures eg., wax seal, signature under selotape or envelopes designed to protect contents.
Faxing	<ul style="list-style-type: none"> Use due diligence to protect against accidental compromise Verify identity of recipient fax before sending. Don't use one touch dialling in case the number has been changed or corrupted 	<ul style="list-style-type: none"> Ideally use email over GSX or encrypted email. Only send once intended recipient has confirmed they are able to collect the fax immediately. 		<ul style="list-style-type: none"> Do not use fax
Printing, Photocopies & Scans	<ul style="list-style-type: none"> Use due diligence to protect against accidental compromise 	<ul style="list-style-type: none"> Only make copies when needed Shred spoilt or extra copies or put in confidential waste bins Collect promptly from the machine Use cross cut shredder or pulp 		<ul style="list-style-type: none"> Only print the number of copies actually needed. Number and log extra copies and register details of those receiving them
Telephones, Conversations & Presentations	<ul style="list-style-type: none"> Use due diligence to protect against accidental compromise 	<ul style="list-style-type: none"> Avoid discussing details in a public place (including taxi's) Do not leave details on voicemail. Remove paper from flip charts & wipe white boards clean before leaving 		<ul style="list-style-type: none"> Do not discuss details in public places or write details on white boards or flip charts.
Electronic Processing	<ul style="list-style-type: none"> Process only on equipment owned or approved by the SNI Support Office (or organisation for lead authorities or parties providing support and maintenance. Use password protected 	<ul style="list-style-type: none"> Use minimum 8 character complex password control Authorise IT accounts on need to know basis Set IT Privileges to 'least privilege' by default Store master copies of files on the 	<ul style="list-style-type: none"> Enforce password protected screensavers to kick in between 5 and 15 mins of non use Use a complex 9+ character password (alpha, numeric & special characters) when applying encryption. 	<ul style="list-style-type: none"> Set system time out to between 15 minutes and 1 hour of non-use. Carry out quarterly system penetration testing

Scottish National Infrastructure
Guideline for Protectively Marking Information

CATEGORY	NONE (IL0)	PROTECT (IL1-2)	RESTRICTED (IL3)	CONFIDENTIAL (IL4)
	screensavers when away from desk.	network <ul style="list-style-type: none"> • Bulk copying & transfers restricted, must be risk assessed & approved by SNI Support Office • Encryption must be used to protect data transfers exceeding 100 personal records • Carry out annual system penetration testing 	<ul style="list-style-type: none"> • Encryption must be used to protect all data transfers 	
E-mail (Internal and External)	<ul style="list-style-type: none"> • Use due diligence to protect against accidental compromise • Take care in addressing email to ensure only intended recipients receive it. • Notify recipients that the email must not be forwarded without the sender's permission. 	<ul style="list-style-type: none"> • Protect content must be in an attachment, not the body of the email itself. • Add protective marking to email subject line • Ideally password protect or encrypt internal email • For external mail, use GSX where available or use 256bit strength FIPS 140 encryption 	<ul style="list-style-type: none"> • GSx permitted for occasional transmission, but not regular use • Apply encryption to any non GSx communications. • Use encryption for internal and external email (irrespective of how many records are enclosed) 	<ul style="list-style-type: none"> • GSx is not to be used for material at this level. Only use encryption.
Other forms of data transfer	<ul style="list-style-type: none"> • Use due diligence to protect against accidental compromise 	<ul style="list-style-type: none"> • Use the secure forms such as GSX, SFTP, HTTPS • Do not use message systems such as Short Messaging Service (SMS) / Multi-Media Messaging Service (MMS) or Instant Messaging (IM) 		
Use of mobile and removable media	<ul style="list-style-type: none"> • Use due diligence to protect against accidental compromise • Place in a lockable drawer when not in use. • Authorised persons are personally responsible for maintaining security • Only remove minimum data necessary 	<ul style="list-style-type: none"> • To be used only in exceptional circumstances & must be authorised by SNI Support Office • A risk assessment of reason for use and data to be stored must be approved by SNI Information Security Officer • Media must be at least 256bit encrypted with a complex 9+ character password with a product accredited to FIPS140-2 • Media must be logged going out and checked and logged back in. 	<ul style="list-style-type: none"> • Removable media must not be used. 	
Mobile working	<ul style="list-style-type: none"> • Use due diligence and protect against accidental compromise • Lock documents & laptops away when not in use eg., car boot, hotel safety deposit box • Do not put portable 	<ul style="list-style-type: none"> • Only use approved equipment • Equipment must use encryption software, (FIPS140), equal to 256 bit strength with a complex 9+ character password (alpha, numeric and special characters) • Logon facilities must be used • Logon and password information must not be written down • Backup electronic records as soon as possible onto the corporate network 	<ul style="list-style-type: none"> • Requires approval from the SNI Support Office & SNI Information Security Officer • Remote access must be over an approved secure mechanism • Paper records must be carried and kept in a secure container or 	

Scottish National Infrastructure
Guideline for Protectively Marking Information

CATEGORY	NONE (IL0)	PROTECT (IL1-2)	RESTRICTED (IL3)	CONFIDENTIAL (IL4)
	computers into aircraft holds.	<ul style="list-style-type: none"> Use lockable containers for paper records 		bag and must not be left unattended at any time.
System Development or Testing	<ul style="list-style-type: none"> Use due diligence to protect against accidental compromise 	<ul style="list-style-type: none"> Risk assess reasons for use and document security controls to be used. Only use real live data only if anonymised data would not guarantee accurate processing. If real data is thought necessary, risk assess using Use of Live Data in Development or Testing which includes a Privacy Impact Assessment Limit the amount of personal data used to the minimum necessary Avoid using Personal Sensitive classified material Place strict exchange, handling and destruction controls on testing body using a Data Sharing Agreement 		
Paperwork	<ul style="list-style-type: none"> Apply a clear desk policy Put documents away when not in use 	<ul style="list-style-type: none"> May be left, face down, on your desk for short periods during the day if protected by one barrier eg., a locked container or room. File away at the end of the day in a locked container. 	<ul style="list-style-type: none"> Protected by two barriers eg., a locked container in a locked room. 	<ul style="list-style-type: none"> Do not leave unattended at any time.
Filing / Archiving	<ul style="list-style-type: none"> Standard office filing and archiving system Store electronic files on the network, not a C drive Identify any statutory retention periods 	<ul style="list-style-type: none"> Ensure records are kept within secure perimeter 	<ul style="list-style-type: none"> Use lockable cabinets or containers If backup tapes are taken off site, use lockable containers for transport and keep logs of transfers. 	<ul style="list-style-type: none"> Store within a Restricted network area Consider separating Personal from Sensitive data to prevent users from seeing all of a record by default
Destruction Methods	<ul style="list-style-type: none"> Follow recycling policy Delete electronic files using standard system facilities 	<ul style="list-style-type: none"> Cross cut shredder or pulp Use confidential waste bins to collect paperwork prior to destruction CD ROMs can be cut into quarters Hard disks must be returned to IT for approved destruction. Use IT approved disk overwrite methods which must involve at least 3 overwrites or degaussing Total destruction of all electronic memory or media and paper to the extent that reconstitution is impossible. Audit data destruction company 		
Markings to be used on documents	<ul style="list-style-type: none"> No marking required Numbering pages is recommended 	<ul style="list-style-type: none"> Indicate the marking level at the top centre of each page. Numbering of pages is essential, and must include number of pages. (eg., Page 1 of 5, 2 of 5....) 		