Central Bedfordshire Council
www.centralbedfordshire.gov.uk

Guidance on Classifications and Protective Markings

April 2017

Security Classification:

Unclassified

Contents:

Classification and Protective Marking FAQ's

What is security classification?

Security classification is a means by which information and the systems that hold that information are grouped so that the same controls around the protection and handling of the information assets can be applied to items with the same classification. Typically security classifications relate to the impact of a loss of confidential information.

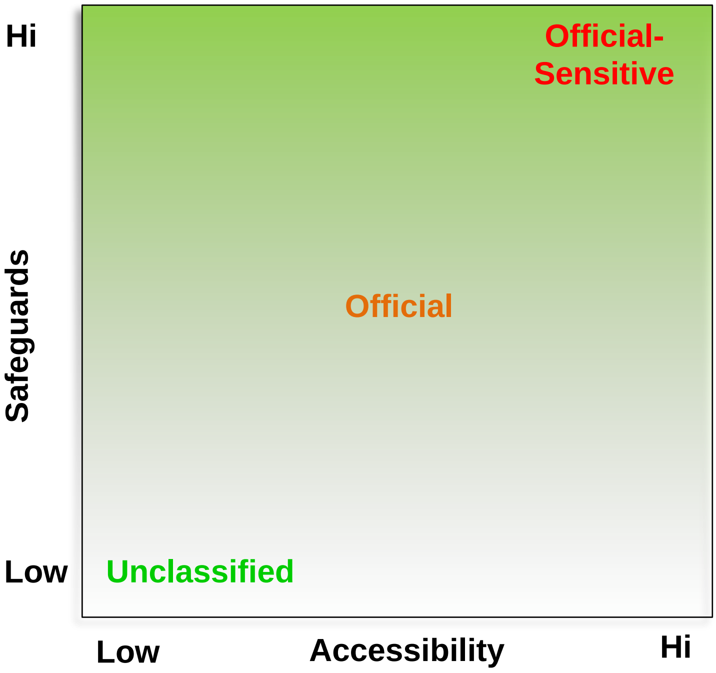
Why classify information at all?

Information is classified in order to ensure that it is protected and handled in an appropriate manner. The Council works with Central Government, other local authorities and a wide variety of public bodies. It is crucial that the public has confidence that the data they supply is handled appropriately and remains secure.

There has been in increased focus on information security, of which classification, protective marking and data handling are part, since the high profile loss of child benefit data by HMRC in 2007. The Information Commissioner's Officer (ICO) was granted new powers in April 2010 to impose fines of up to £500,000. The ICO publish a list of actions that they have taken under the Data Protection Act when breaches have come to light (See ICO Enforcement Actions). In November 2010 the ICO fined a local authority £100,000 for two serious breaches of the Data Protection Act.

Implementing rigorous data handling practices is a key element in demonstrating due diligence to the ICO and will be taken into account as a defence if a breach occurs. The physical, administrative and technical controls used to safeguard information relate directly to its classification. Due to the cost of safeguards it is important to apply these only where they are genuinely required.

Applying classifications ensure that the appropriate safeguards are applied where they are needed and saves the cost associated with applying safeguards where they are not required. In terms of confidentiality, the safeguards for more highly classified information will tend to make information available to fewer people based on their need to use it. The appropriate data handling procedures to use are indicated by the protective marking.



If the information if not protectively marked then it is far less likely to be handled appropriately.

When is information classified?

A decision on the security classification that information is given needs to be made when the information is originally created or collected. For a business as usual process, such as completing a pro forma, the classification decision can be once, in advance and inserted on to the blank pro forma (template) by appending ‘WHEN COMPLETED’ to the protective marking.

For example, when designing a pro forma to collect personally identifiable information it can have ‘OFFICAL WHEN COMPLETED’ pre-printed. Similarly, if the form were designed to collect personal sensitive data it should have ‘OFFICIAL-SENSITIVE WHEN COMPLETED’ pre-printed.

How to classify material originating outside of HMG?

Outside HMG there is no agreed UK system for marking sensitive material, although terms such as PRIVATE or CONFIDENTIAL are in common use, particularly in relation to personally identifiable information. Any material originating outside of government, that is not covered by recognised protective marking, an international agreement, contract or other agreement, but is marked in such a way to indicate sensitivity must, when handled, be protected to at least the level officer by the protective marking, and a higher marking should be considered.

How do I make the classification decision?

All items containing personal information or sensitive personal information should have a security classification applied. The key difference between the Official-Sensitive and Official classifications is the impact of the unauthorised disclosure of the information:

Official – would cause some distress to a limited number of individuals

Official-Sensitive – would cause substantial distress to a large section of the community or have a detrimental impact on the running of CBC

Careful consideration should be given as to whether aggregates of information should be classified at a higher level due to the greater impact of loss of the information. The Cabinet Office recommends that 1000+ personal records be afforded a higher classification when aggregated.

What is personal data?

Personal data is defined in the Data Protection Act 1998 and European Data Protection Directive (95/46/EC) as identifying, or relating to, an identifiable living individual.

In most cases it will be clear when personal data is being stored or processed. In those few cases in which it is unclear please see ‘Data Protection Technical Guidance: Determining what is personal data’ available on the ICO’s website. Alternatively you can consult the Councils Data Protection Officer.

Personal data should be classified as OFFICIAL.

See What is personal data? – A quick reference guide for more information.

What is sensitive personal data?

Sensitive personal data is defined in the Data Protection Act 1998 as information about a data subject and includes the following:

- Racial or ethnic origin
- Political opinions
- Religious or Other Similar beliefs
- Membership of a trade union
- Physical and mental health
- Sexual / Personal life
- Alleged or proven criminal or civil offences

Sensitive personal data should be classified as OFFICIAL-SENSITIVE.

How should I mark different types of information?

The practicalities of marking different types of information require different practices to be used:

- Hard copy (printouts) – the security classification is to be printed in capitals in the header or footer of every page of the document

- Hard copy (received) – when labelling existing hard copy that does not already have a protective marking, you may label only the first page or cover

- Removable media (e.g. diskettes, CD-Rs, tapes) – attach a sticker to the media. Please note it is not necessary to protectively mark encrypted memory sticks

- Electronic records – a classification should be added where is will be clearly visible

Can I assume that is a document is unmarked it is public?

Whilst it is good practice to mark information as ‘UNCLASSIFIED’ if it does not need a protective marking there will be instances where this has not been done. If you intending to disclose the document you should first:

- Check with the author of the document, where possible

- Carefully read through the information to ensure that it does no contain information to indicate that is should have a protective marking rather than being public

- Ask your line manager or the Councils Data Protection Officer for advice

What should I do about classifications that I do not recognise?

Where partner organisations or individuals do not use the GPMS or the CBC marking schemes you should interpret markings such as ‘CONFIDENTIAL’, ‘IN CONFIDENCE’ or ‘PRIVATE’ to indicate that the information needs to be handled as ‘OFFICIAL’ at least. If in doubt you should consult your line manager.

How do classification and protective marking relate to handling procedures?

Different classifications of information will have different handling procedures. It is the handling procedures that provide a level of control commensurate od the risk of inappropriate disclosure. The handling procedures apply to the full lifecycle of the information, from its creation to destruction. Table 1 outlines the controls for printed information and Table 2 outlines the controls for electronically held information.

How does classification relate to clear desk and clear screen policies?

Having a clear desk and a clear screen are two of the controls that relate to the handling of ‘OFFCIAL’ and ‘OFFICIAL-SENSITIVE’ information. If you are away from your desk you should ensure that any information, that has one of these protective markings, is secure. You should also ensure that you your screen so that no one else is able to access the any protectively marked information that you may have previously accessed with your login credentials.

What precautions do I need to take with email?

When sending a new email that needs to be protectively marked, you should type ‘OFFICIAL’ or ‘OFFICIAL-SENSITIVE’ into the subject line before the email subject. Do not use the Outlook sensitivity settings ‘Private, Personal and Confidential’ as these are not the protective markings adopted by CBC (or HMG) for security classifications.

Be careful when ‘replying to all’ as this will send a message back to everyone listed in the To: and CC: fields. Some of these people may not need to see your reply and some may be external parties. If you reply to all without checking for recipients with external email addresses, your reply could be routed insecurely over the internet.

Please see the ‘Secure Email Guidance’ document on the Information Security page on the intranet for more information.

Where can I find additional official guidance on data protection and data handling?

There are a number of online resources that you can use to find out more about data protection and data handling:

Local Government Data Handling Guidelines

Security Policy Framework

Information Commissioners Office

The Council has obligations to data subjects under the Data Protection Act 1998:

Data Protection Act 1998

Principle 7 – Information Security

Free training on protecting information is published at:

The National School of Government Protecting Information Courses

Table 1 – Safeguards for Printed Information

	OFFICIAL-SENSITIVE	**OFFICIAL**	**UNCLASSIFIED**
Creation/Receipt	Number each page Protectively mark each page Protectively mark front cover (received items)	Number each page Protectively mark each page Protectively mark front cover (received items)	Number each page Protective marking is recommended[1]
Storage/Retention	Store hard copy under lock and key	Store hard copy under lock and key	No restrictions
Removal from Site	Must not be removed from site	Must be stored under lock and key while in transit or temporarily off sight	No restrictions
Copying	Do not copy Official-Sensitive information without the approval of its owner	Official information should only be copied when absolutely necessary	Normal restrictions apply to copyrighted material
Transfer	If the information is also available in electronic form, and can be received electronically, it should not be sent as hard copy. Hard copy should be sent using door to door courier, be hand delivered or sent via a method that can be tracked at every step i.e. special delivery. Confirmation of receipt should be sought	If the information is also available in electronic form, and can be received electronically, it should not be sent as hard copy Hard copy should be sent using door to door courier, be hand delivered or send via a method that can be tracked at every step i.e. special delivery. Confirmation of receipt should be sought	No restrictions
Disposal	Hard copies must be cross cut shredded or placed in the confidential waste bins	Hard copies must be cross cut shredded or placed in the confidential waste bins	No restrictions

Table 2 - Safeguards for Electronic Information

	OFFICIAL-SENSITIVE	OFFICIAL	UNCLASSIFIED
Creation/Receipt	Number each page Protectively mark each page	Number each page Protectively mark each page	Number each page Protective marking recommended[1]
Storage/Retention	Never store on an area of the network that is 'shared' or 'public'	Never store on an area of the network that is 'shared' or 'public'	No restrictions
Removal from Site	Do not remove information from site unless absolutely necessary and then only on encrypted removable media	Do not remove information from site unless absolutely necessary and then only on encrypted removable media	No restrictions
Copying	Do not copy Official-Sensitive information unless absolutely necessary Only copy to a secured network or onto encrypted removable media[3]	Official information should only be copied when absolutely necessary Only copy to a secured network or onto encrypted removable media[3]	No restrictions
Transfer	If transferred to another organisation this must be sent using encrypted email or removable media[2]	If transferred to another organisation this must be sent using encrypted email or removable media[2]	Normal restrictions for copyrighted material
Disposal	All removable media should be returned to IT for sanitisation and secure disposal	All removable media should be returned to IT for sanitisation and secure disposal	No restrictions

Notes:

1. It is good practice to mark information with its classification to avoid doubt
2. Use the encryption features within WinRAR rather than MS Office. 'Password to Open' feature must not be used to protect data transferred within CBC. SFTP, MessageLabs Policy Based Encryption or Office 365 Encryption services should be used to transfer data outside the council
3. Publically accessible internet sites are not secure and therefore information classified as OFFICIAL-SENSITIVE or OFFICIAL must not be published or copied to such sites

Central
Bedfordshire

A great place to live and work

Contact us…

by telephone: 0300 300 8XXX
by email: customer.services@centralbedfordshire.gov.uk
on the web: www.centralbedfordshire.gov.uk
Write to Central Bedfordshire Council, Priory House,
Monks Walk, Chicksands, Shefford, Bedfordshire SG17 5TQ