
Warwickshire County Council



Information Security

Protective Marking, Handling and Disposal Policy

This document's security classification is NOT PROTECTIVELY MARKED

Document Control

Title: Protective Marking Policy
Issued by: Corporate Information Management
Date: 26th March 2010
Author: Andrew Morrall, Corporate Information Manager
Status: Version 3

Revision History

Version	Originator	Summary of Changes	Date
1.0	Andrew Morrall	Released following approval by SDMT	26/09/2006
2.0	Andrew Morrall	Revised to include new Protect level and Disposal policy, approved by ISF	07/11/2008
3.0	Andrew Morrall	Revised Appendix A in line with HMG IA Standard No. 1 Business Impact Tables. Revised Appendix B to simplify. Revised Appendix C to clarify electronic handling	26/03/2010

Approvals

This document requires the following approvals before release.

Name	Title/Role
Les Harlock	ICT Security Manager
ISF	Information Security Forum
Kushal Birla	Head of Customer Service and Communications

Table of Contents

- 1. INTRODUCTION 4**
- 2. PURPOSE 4**
- 3. SCOPE 4**
- 4. ENFORCEMENT 4**
- 5. RELATED DOCUMENTATION 4**
- 6. POLICY 5**

- APPENDIX A – RISK AND IMPACT ASSESSMENT 7**
- APPENDIX B – PROTECTIVE MARKING DESCRIPTORS 8**
- APPENDIX C – HANDLING, STORAGE, AND DISPOSAL PROCEDURES 9**

1. Introduction

The Authority needs to protect information securely in line with the sensitivity of content and risk of disclosure.

By using the Government standard marking scheme, the information will be labelled, stored, handled and disposed of, in accordance with relevant legislation and Government standards.

2. Purpose

The policy defines how information used within the Authority is to be security marked, handled and disposed of, for both paper and electronic media.

The Protective Markings do not impose any classification to restrict or to supply information under the Freedom of Information Act, Data Protection Act or Environmental Information Regulations. However, they may indicate that all or some of the information may be subject to exemptions, for example personal information.

3. Scope

This policy applies to:

- All permanent employees;
- All temporary/contract employees employed or engaged by the County Council;
- Workers/volunteers employed or engaged by the County Council;
- All employees of partner or subsidiary organisations whilst at work and/or engaged on County Council business;
- Councillors when using IT equipment supplied by the County Council;
- Any other authorised users.

Any reference in this document to “employee” is deemed to be a reference to any of the foregoing

4. Enforcement

The policies and security requirements in this document refer to and gain authority from the WCC Information Security Policy statement as authorised and issued by the WCC Chief Executive.

Applicability, and therefore enforcement, extends to anyone who is subject to the WCC Information Security Policy Statement and who undertakes activities governed by this Policy.

5. Related Documentation

This policy refers to and should be read in conjunction with the following documents:

Document Description	Type
Responsibility for Information Assets	Information Security Policy
Encryption Standard	Information Security Policy
Clear Desk and Clear Screen Policy	Information Security Policy
Records Management Policy	Information Policy
Information Sharing Charter and Protocols	Information Policy

6. Policy

Protective Marking

- 6.1 All information for **internal and partner** use will be protectively marked using the agreed markings detailed within this policy and must be used by all employees.
- 6.2 Employees must assess all information for a protective marking using the impact assessment in Appendix A, based on risk and impact of disclosure.
- 6.3 The protective markings to be used by employees are:

NOT PROTECTIVELY MARKED

Anyone can access the information internally or externally. It may be published on the web or in paper form (but may still be copyright and chargeable).

Where it has a purpose or adds value, the markings will be “NOT PROTECTIVELY MARKED”, otherwise there will be no markings on the information or document.

PROTECT

Information where disclosure or unauthorised access would be inappropriate, inconvenient or cause harm or financial impact.

There will be clear markings on the information as “PROTECT”.

RESTRICTED

Information to be restricted at a higher level of assurance than Protect, due to significant inconvenience, damage, harm or financial impact on the Authority or individuals. This marking applies to the holding, storage and transmission of bulk customer or employee records and access will be restricted.

There will be clear markings on the information as “RESTRICTED”.

- 6.4 Descriptors listed in Appendix B must be used for PROTECT and RESTRICTED information to describe the reason for the protection and restriction.
- 6.5 All PROTECT and RESTRICTED information must be marked at the centre top or bottom of each page, with the relevant marking.
- 6.6 Protective markings must be reviewed during the life of the information or document to ensure the marking is appropriate and relevant. For example:

A policy or management decision may be in draft form and marked “PROTECTED - MANAGEMENT”, but once ratified it may become available to all and the marking removed.

Handling

- 6.7 All information must be stored and handled appropriate to its protective marking, as detailed in Appendix C.
- 6.8 Employees must not attempt to handle, store or transmit information by any means other than that defined for each Protective Marking within this policy Appendix C.
- 6.9 Transfer or transmission of RESTRICTED information must be authorised by the Information Asset Owner or delegated officer.
- 6.10 If employees receive or handle information that is marked by a more secure Government Protective Marking of CONFIDENTIAL, SECRET and TOP SECRET, they must discuss the issue immediately with Information Security who will advise.

Disposal

- 6.11 All information must be disposed of or sent to archive, in accordance with an approved retention and disposal schedule as part of the WCC Records Management Policy.
- 6.12 The destruction of information must be appropriate to its protective marking as detailed in Appendix C.
- 6.13 All redundant copies of WCC information classified as 'Protect' or 'Restricted' or above that has been generated in the course of printing, photocopying or handling such information, must be destroyed according to approved procedures.
- 6.14 It is the responsibility of the Information Asset Owner to ensure that procedures are followed to assure secure disposal of information when it is no longer required.
- 6.15 Where destruction of 'Protect' or 'Restricted' WCC information is given to a third party, this must be carried out by authorised WCC personnel or a WCC approved external destruction service.
- 6.16 When a third party is used for the disposal of WCC information, the third party must be contractually bound to employ security controls required by WCC.
- 6.17 Destruction of 'Protect' or 'Restricted' WCC information captured on electronic storage media must only be performed with methods and equipment approved by Information Security.
- 6.18 All data and software on WCC information system hardware or machine-readable media will be erased and made unrecoverable prior to reuse within the Council.
- 6.19 All data and software on WCC information system hardware or machine readable media will be erased and made unrecoverable prior to release to a third party for disposal, sale, service or repair.
- 6.20 WCC asset registers will include any devices that have been taken from service, sent for repair, used for parts or destroyed.

Policy Review

- 6.21 The Corporate Information Manager will ensure that this policy is up-to-date and relevant.

Appendix A – Risk and Impact Assessment

The table below defines how the information content in WCC is assessed for risk and impact to determine the appropriate Protective Marking.

The **Impact Levels** refer to HMG Business Impact Tables defined in HMG IA Standard 1.

Impact if the data is disclosed, lost or stolen and misused	Protective Marking	Examples	Impact Level
<ul style="list-style-type: none"> • Little or no impact on the finances of the Authority • No inconvenience or distress to the customer • Little or no financial impact to the customer • Little or no impact on the Authority's standing or reputation. 	NOT PROTECTIVELY MARKED	<ul style="list-style-type: none"> • Policies and procedures • Documents available in the public domain or on the WCC public website • Property address where it does not identify the individual owner or residents • Names and contact details of specific employees or individuals that are in the public domain or an individual has authorised 	0 or 1
<ul style="list-style-type: none"> • Short-term inconvenience, harm or distress to an individual • Cause financial loss or loss of earning potential, or to facilitate improper gain • Damage to the Authority's standing or reputation • Financial impact to the Authority (upto £1M) • Breach proper undertakings to maintain the confidence of information provided by individuals or third parties • Breach statutory restrictions on the disclosure of information 	PROTECT	<ul style="list-style-type: none"> • Personal information relating to any customer or employee such as a name, address and contact details, VAT number or National Insurance number for which we have a duty of care. • Exempt Committee papers excluded from the public under Local Government Act • An employee record • A customer case file • Draft documents before approval for release into public domain 	2
<ul style="list-style-type: none"> • Substantial inconvenience, harm or distress to individuals • Cause financial loss or loss of earning potential, or to facilitate improper gain or advantage • Substantial damage to the Authority's standing or reputation • Significant Financial impact to the Authority (£Millions) • Prejudice the investigation of or facilitate the commission of low-level crime, hinder detection of serious crime • Could have wider implications within government • Affect diplomatic relations 	RESTRICTED	<ul style="list-style-type: none"> • Complete set of an individual's social care files or health record • Investigation files • A smaller multiple of complete customer/employee records where information is sensitive, or has financial or identity data (remembering that the marking reflects the highest impact individual item) • Volumes of "Protect" data about a reasonably large number (hundreds) of customers or employees 	3

Appendix B – Protective Marking Descriptors

The table below defines how a descriptor may be used with the marking based on information content. For example, PROTECT – PERSONAL. They are not mandatory. The descriptors also serve to help those handling the information to decide which people should have access to the material. Information received from public sector partners may use one of these descriptors. You may receive information marked with one of these descriptors. You can also add your own local caveats in addition, to aid understanding.

Descriptor	
APPOINTMENTS	Actual or potential appointments yet to be announced
COMMERCIAL	Disclosure would be likely to damage a third party or commercial establishment's processes or affairs
CONTRACTS	Tenders in progress and contract terms accepted
FOR PUBLICATION	Information is planned to be published at a future date (when it will change to NPM)
HONOURS	Unannounced recognitions
INTERNAL	Only available to WCC employees and should not be published or circulated outside of WCC without permission
INVESTIGATIONS	Investigations into disciplinary affairs or may lead to criminal cases
LOCSEN	Locally sensitive issues not yet for publication
MANAGEMENT	Policy and planning affecting the interests of the Authority or staff
MEDICAL	Medical reports, records and material relating to an individual
PERSONAL	Information that is personal to an individual or the sender and/or recipient
REGULATORY	Limited by existing regulation
STAFF	Contains references to named or identifiable staff or personal confidences entrusted by staff to management

Appendix C – Handling, Storage, and Disposal Procedures

The table below defines how the information resource can be handled, transmitted, stored and disposed for the different security protective markings in use by the Authority.

Internal applies for sending information within WCC, **External** applies for sending information outside of WCC to partners or third parties. Do not use a marking on correspondence sent to the public.

Handling

	NOT PROTECTIVELY MARKED	PROTECT	RESTRICTED
Document Marking	“NOT PROTECTIVELY MARKED” at the centre top or bottom of every page, when applicable.	“PROTECT[descriptor]” at the centre top or bottom of every page.	“RESTRICTED [descriptor]” at the centre top or bottom of every page.
Email	<ul style="list-style-type: none"> WCC internal email, internet email or Government secure email 	<p>Internal:</p> <ul style="list-style-type: none"> WCC email marked PROTECT in the subject line using the disclaimer Only to be opened by addressee(s) or delegated employee Seek permission of the sender before forwarding or sending to other addresses <p>External using GC:</p> <ul style="list-style-type: none"> Secure email marked as above using Government Connect Secure Email if available for public sector partners. <p>External using internet:</p> <ul style="list-style-type: none"> Encrypt information in an attachment Only use if the sender needs a reply, you are sure who is receiving it, and they consent to a reply via internet email. 	<p>Internal:</p> <ul style="list-style-type: none"> WCC email marked RESTRICTED in the subject line plus relevant disclaimer of “Restricted” inserted. Only to be opened by addressee(s) Never forward or send to other addresses <p>External using GC:</p> <ul style="list-style-type: none"> Secure email marked as above using Government Connect Secure Email if available for public sector partners, or encryption if not available. Encrypt any volume data in an attachment <p>External using internet:</p> <ul style="list-style-type: none"> Never send via internet email

Electronic transmission and media	<ul style="list-style-type: none"> • Any 	<ul style="list-style-type: none"> • Secure, approved connection as agreed by Information Security, or encrypted data to WCC Encryption Standard 	<ul style="list-style-type: none"> • Secure, approved connection as agreed by Information Security, or encrypted data to WCC Encryption Standard. • Transmission/transfer only to take place with the approval of the Information Asset Owner or delegated employee.
Public Website	<ul style="list-style-type: none"> • Can be used with uncontrolled or open access. 	<ul style="list-style-type: none"> • Only to be used with authenticated access. 	<ul style="list-style-type: none"> • Only to be used with authenticated access.
Post	<ul style="list-style-type: none"> • Internal or external mail. 	<p><u>Internal:</u></p> <ul style="list-style-type: none"> • Sealed envelope marked “PROTECT Addressee Only”. • Only to be opened by addressee or delegated employee. <p><u>External:</u></p> <ul style="list-style-type: none"> • Sealed envelope using Royal Mail marked “Private and Confidential” where appropriate. If important or highly sensitive consider using ‘Recorded Signed For’ service. 	<p><u>Internal:</u></p> <ul style="list-style-type: none"> • Sealed envelope marked “RESTRICTED Addressee Only”. • Only to be opened by addressee or delegated employee. <p><u>External:</u></p> <ul style="list-style-type: none"> • Sealed envelope marked “RESTRICTED” contained within a package with no protective markings. • Use of secure courier to named person or delivery by hand.
Telephone	<ul style="list-style-type: none"> • Internal, public network, mobile 	<ul style="list-style-type: none"> • Normal use if recipient can be identified and spoken to. • Inform the recipient that the information is protected. • Do not leave messages on answering systems. 	<ul style="list-style-type: none"> • Normal use if recipient can be identified and spoken to. • Inform the recipient that the information is restricted. • Do not leave messages on answering systems.
Fax	<ul style="list-style-type: none"> • Normal fax 	<ul style="list-style-type: none"> • Recipient must be at hand. • Send cover sheet first and wait for confirmation before sending. 	<ul style="list-style-type: none"> • Do not use

<p>Mobile - home or working away from office</p>	<ul style="list-style-type: none"> • Normal WCC 	<ul style="list-style-type: none"> • Do not leave unattended. • Secure assets out of sight and locked away when not in use. • Information must not be discussed in a public place where it may be overheard. • Not to be stored electronically on personal home computer or personal mobile device. • Minimum encryption protected on WCC mobile storage device. • Remote access to server based master is preferable. • Personal use only, no access to unauthorised users. <p>See “storage of papers” and “electronic storage” procedures above for procedure when away from office or at home.</p>	<ul style="list-style-type: none"> • Only if approved by the Information Asset Owner • Never leave unattended. • Secure assets out of sight and locked away when not in use. • Information must not be discussed in a public place where it may be overheard. • Not to be stored electronically on personal home computer or personal mobile device. • Minimum encryption protected on WCC mobile storage device. • Remote access to server based master is preferable. • Personal use only, no access to unauthorised users. <p>See “storage of papers” and “electronic storage” procedures above for procedure when away from office or at home.</p>
---	--	--	---

Storage

	NOT PROTECTIVELY MARKED	PROTECT	RESTRICTED
Storage of papers	<ul style="list-style-type: none"> • Normal WCC 	<ul style="list-style-type: none"> • Protected by one physical lock. Examples: locked drawer or cabinet. 	<ul style="list-style-type: none"> • Protected by two physical locks. Examples: locked safe and office.
Electronic storage	<ul style="list-style-type: none"> • Normal WCC or unencrypted mobile devices 	<p>WCC network:</p> <ul style="list-style-type: none"> • Controlled access by defined user groups to specific areas. For example: network storage, electronic document management systems, application systems. <p>Mobile working:</p> <ul style="list-style-type: none"> • Encrypted to minimum WCC encryption, preferably access directly through remote network access. Examples: Secure fob and Citrix. • Do not leave screen unattended. (See also Mobile Working) 	<p>WCC network:</p> <ul style="list-style-type: none"> • Controlled access by defined user groups to specific areas. For example: network storage, electronic document management systems, application systems. <p>Mobile working:</p> <ul style="list-style-type: none"> • Encrypted to minimum WCC encryption, preferably access directly through remote network access. Examples: Secure fob and Citrix. • Do not leave screen unattended. (See also Mobile Working)
Electronic backup	<ul style="list-style-type: none"> • Backup stored in locked cabinet. 	<ul style="list-style-type: none"> • Backup stored in locked cabinet. 	<ul style="list-style-type: none"> • Backup stored in locked cabinet.

Disposal

	NOT PROTECTIVELY MARKED	PROTECT	RESTRICTED
Disposal of papers	<ul style="list-style-type: none"> • Recycle 	<ul style="list-style-type: none"> • Secure waste disposal – destruction or shredding. 	<ul style="list-style-type: none"> • Secure waste disposal – destruction or shredding.
Electronic media disposal	<ul style="list-style-type: none"> • Normal deletion and reuse. 	<ul style="list-style-type: none"> • Destruction or erased to make unrecoverable if for reuse. 	<ul style="list-style-type: none"> • Destruction or erased to make unrecoverable if for reuse.