

Classification Policy

Name: Classification Policy

Version: 1.7

Issue Date: 08/07/2003



File	Classification Policy	Pages	1	Version	1.7
Owner	John Pritchard	Distribution	ICT & MRU	Classification	Unclassified

Document Control

This is a CONTROLLED document and updates or changes to this document are authorized and then advised by email to the relevant document holders.

It is UNCONTROLLED when printed. You should verify that you have the most current issue.

DOCUMENT HISTORY

Author(s)

Names	Role
John Pritchard	ICT Enterprise Architecture Manager

Document Log

Version	Status	Date Issued	Description of Change	Pages affected	Review
1.0		08/07/2003	Approved and adopted by the Chief Executive Management Team (CXMT)		
1.1	Final	11/10/2007	Updated & Reviewed		October 2008
1.2	Final	01/10/2007	Updated & Reviewed		October 2009
1.3	Final	08/12/2008	Document moved to corporate policy template	All	
1.4	Final	18/12/2008	Updated to reflect guidance from central government	All	
1.5	Final	09/02/2009	Updates Following ICT Consultation	All	
1.6	Final	09/05/2010	Change of Ownership	All	01/04/2011
1.7	Final	15/06/2011	Reviewed	All	May 2012

File	Classification Policy	Pages	2	Version	1.7
Owner	John Pritchard	Distribution	ICT & MRU	Classification	Unclassified

Contents

Contents

<u>Classification System</u>	5
<u>Classification Labelling</u>	5
<u>Degree of Risk</u>	6
<u>Risk</u>	7
<u>Changes in Classification and Retention of Data</u>	7
<u>Classification Guidelines</u>	8
<u>Data Types and Classification Examples</u>	8
<u>Classification Handling Criteria</u>	11
<u>Classified Data</u>	11
<u>Photocopying</u>	12
<u>Physical Protection</u>	12
<u>Security of Media in Transit</u>	12
<u>Unified Classification Markings</u>	13
<u>Interoperability between Organisations</u>	13

File	Classification Policy	Pages	3	Version	1.7
Owner	John Pritchard	Distribution	ICT & MRU	Classification	Unclassified

Purpose of this policy

Information has varying degrees of sensitivity and criticality. Security classification of information is therefore required to ensure that the information processed within Herefordshire Council 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 and the value of classification is lost becoming, by over use, commonplace. 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 organisations, and to their, future of not applying the classification system intelligently.

The purpose of this Classification Policy is to provide the method of how information is handled and protect against the risk of unauthorised disclosure.

Unauthorised disclosure is the disclosure of information either accidentally or deliberately to an individual or facility i.e. the Internet who is not authorised to view the information. 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 is Confidential. 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.
- This updated policy incorporates the requirements of Government Connects within the classification policy, to enable the Council to use the Government Secure Email Service.

Who does this policy / procedure / protocol apply to?

This policy applies to anyone with access to Herefordshire Council, including but not limited to employees, Councillors and 3rd party contractors.

File	Classification Policy	Pages	4	Version	1.7
Owner	John Pritchard	Distribution	ICT & MRU	Classification	Unclassified

1. Classification System

Too many classes should be avoided and usually two levels are adequate. It is therefore proposed that the examples below are adopted and implemented throughout Herefordshire Council.

Restricted

This applies to information that originates from the Customer Information System (CIS) system and any data that can only be sent over a Government Secure Intranet connection.

Protect

May more commonly referred to as confidential. A document that is intended for the recipient only. It must be labelled, numbered and accounted for. It should never be copied without the originators permission, must be kept in secure conditions and shredded when discarded.

Such documents would, if made available to competitors, have an adverse effect on the organisation's future. They must be labelled with paper copies limited to those with specific need to know. Documents must be shredded when discarded. Computer files must be protect by password controls.

Unclassified

These are documents generated and used daily for routine communication and require no special handling requirements.

2. Classification Labelling

Classification labelling applies to all forms of information both hard copy (paper) and electronic data including e-mail originated within Herefordshire Council. All magnetic media, which includes servers, floppy disks, CD ROMs, hard drives, removable hard drives etc must be labelled commensurate with their contents.

Protect

All hard copy data will be franked top and bottom e.g. PROTECT. Data processed electronically will bear the classification markings in the document header and footer. Data with a protect classification must be transferred using the Government Connects system or encrypted to the current Council required level. If you are unsure always seek guidance from the information security team before sending Potentially Protect data.

File	Classification Policy	Pages	5	Version	1.7
Owner	John Pritchard	Distribution	ICT & MRU	Classification	Unclassified

Unclassified

This is data, which does not require marking.

3. Degree of Risk

Classified information is protectively marked so that people know how to apply the appropriate security protection. The classification is dependant upon the impact or damage likely to occur if the information was leaked or disclosed to the wrong people. The table below shows the degree of risk afforded to the unauthorised disclosure of the above classification levels:

File	Classification Policy	Pages	6	Version	1.7
Owner	John Pritchard	Distribution	ICT & MRU	Classification	Unclassified

Classification	Risk
Restricted	Is applied to information from the CIS system. And all due care should be taken to protect this information by officers.
Protect	Information whose unauthorised disclosure (even within Herefordshire Council) would cause serious damage to the interests of the Council. It would normally inflict harm by virtue of serious financial loss, severe loss of profitability or opportunity, grave embarrassment or loss of reputation.
Protect (Personal)	When handling one individuals personal data.
Protect (Private)	When handling more than one individuals personal data.
Protect (Commercial)	For use on document/information that is contract or information that may harm the commercial interests of the Council or a third party
Protect (Management)	Should be used for draft policies etc and other information that may harm the management of the Council or 3 rd parties should it be released
Unclassified	These are documents generated and used daily for routine communication and require no special handling requirements.

4. Changes in Classification and Retention of Data

Classification of data can change in relation to the circumstances in which the data was originated. An example might be classified budgetary information or information relating to redundancy information which would be Protect during origination and formulation. Once this information has been released into the public domain it would become unclassified and require downgrading.

The classification of data therefore requires regular reviews. 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 Herefordshire Council's Record Retention Schedules.

File	Classification Policy	Pages	7	Version	1.7
Owner	John Pritchard	Distribution	ICT & MRU	Classification	Unclassified

5. 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 Herefordshire Council 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 protect? Any originator who has problems with the classification of data should consult their line manager.

6. Data Types and Classification Examples

The table below (the list is not exhaustive) provides guidelines and examples of different types of data with a suggested classification. It should be noted that even if information is marked as protect it may still be releasable under the Freedom of Information Act.

File	Classification Policy	Pages	8	Version	1.7
Owner	John Pritchard	Distribution	ICT & MRU	Classification	Unclassified

	Classification	Data Content
Any	Protect	<ul style="list-style-type: none"> Open correspondence between Herefordshire Council and others. Data relating to Confidential issue negotiations between firms tendering for contracts. Data relating to prices and contracts.
ICT Information	Protect	All passwords, Combination settings and Security Keys.
Finance data	Unclassified	Normal financial data of a non-controversial nature, which could be in the public domain.
	Protect	Financial data relating to budgets and or corporate projects under review by Senior Executive Management Team.
Legal documents	Unclassified	Standard legal correspondence not relating to client details.
	Protect	<ul style="list-style-type: none"> Client information relating to litigation and/or proceedings. Names, addresses and dates of birth of Herefordshire Council employees.
Personnel	Unclassified	Standard day-to-day business meetings and minutes.
	Protect	Personal sensitive data as stated in the Data Protection Act 1998 relating to: <ul style="list-style-type: none"> Racial or Ethnic origin Political opinions, religious or other beliefs of a similar nature Trade union membership Physical or mental health or condition Sexual life Offences (including alleged offences) Criminal proceedings
Child/Client data	Unclassified	Advertising e.g. Clubs, services and voluntary groups.
	Protect	<ul style="list-style-type: none"> Names, addresses and dates of birth of Herefordshire Council employees. Children and Adults personal educational data
Environment	Unclassified	Standard day to day administration
	Protect	<ul style="list-style-type: none"> Lists of children on Provision Bus routes Some Planning Applications

File	Classification Policy	Pages	9	Version	1.7
Owner	John Pritchard	Distribution	ICT & MRU	Classification	Unclassified

Social Care and Strategic Housing	Unclassified	Standard day to day administration
	Protect	<ul style="list-style-type: none"> Names, addresses and dates of birth of Herefordshire Council employees. Personal client information concerning child abuse etc.
GSI (Government Secure Intranet) Information	Restricted	<ul style="list-style-type: none"> Any information that is sent over GSI should be protected or restricted and this must be classified appropriately in the email subject Restricted data is any data where it is mandated that the Council must use a GSI account to transmit the data.

File	Classification Policy	Pages	10	Version	1.7
Owner	John Pritchard	Distribution	ICT & MRU	Classification	Unclassified

7. Classification Handling Criteria

The table below details the handling criteria for all Protect Data:

	Classified Data
User Access Limitations	<ul style="list-style-type: none"> • Access limited to authorised data users on a need to know basis • Access to IT management systems is limited to authorised hierarchical constraints • Standard password requirement • Individual files may also be password protect at the discretion of the originator
Transmission Restrictions E-Mail	<ul style="list-style-type: none"> • Transmission from and to the Internet requires encryption • Transmission across all areas of the Intranet and internally requires encryption
Waste Disposal: Printed Format	Cross Cutting Shredded or Incinerated
Waste Disposal: IT Media	<ul style="list-style-type: none"> • Floppy disks and CDs destroyed by Shredding • Hard Drives degaussed as arranged by ICT Services only • Certificates must be raised confirming the cleansing of hard drives • USB Devices must be handed to ICT Services for Secure Destruction, this will be completed by a security clear partner organisation
Home Working	To be approved by the Directorate ICT Client Officer within the constraints of the Authority's Home Working Procedures
Mobile Working	To be approved by the Directorate ICT Client Officer within the constraints of the Authority's Home Working Procedures
Facsimile (Fax)	<ul style="list-style-type: none"> • Authentication of reception before transmission is required. • Confirmation of receipt is required. • Pre-programmed telephone numbers entered to prevent miss dialling. • Regular checks must take place to ensure that numbers have not changed.

File	Classification Policy	Pages	11	Version	1.7
Owner	John Pritchard	Distribution	ICT & MRU	Classification	Unclassified

8. Photocopying

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.

9. Physical Protection

The physical protection of protect documents is comparatively simple. There are many fire proofed document containers available that offer good thief resistance. They range in size from dispatch box to full cupboard size and may be locked by either combination or keyed locks. Inbuilt alarm systems can be incorporated and these can be programmed to record all access to the documents.

Any classified document should, without fail, be accounted for by signature and after the working day be secured as above. A clear desk policy should be strictly enforced at all times.

10. Security of Media in Transit

The physical protection of protect documents in transit can be similarly protect and large offices should operate a messenger system with locked keys. The originator and the recipient hold the keys only.

Envelopes containing classified documents should be clearly marked with the classification so that persons other than the intended level of recipient do not open it. If documents are to be carried by Public Carriers a second, outer envelope should be used showing destination address only and no indication of document classification. In addition the following procedures must be applied:

- Only reliable transport services should be used. A list of preferred couriers should be compiled and maintained within each service area. It is the head of service responsibility to maintain this list. Advice on how to pick appropriate secure suppliers can be provided by ICT Services.
- Procedures for checking a courier's identity should be implemented.
- Packaging of data should be sufficient to protect it from physical damage.
- Special controls such as the use of locked containers, delivery by hand and tamper evident packaging should be used to further protect classified information from unauthorised disclosure.

File	Classification Policy	Pages	12	Version	1.7
Owner	John Pritchard	Distribution	ICT & MRU	Classification	Unclassified

11. Unified Classification Markings

Many organisations already have an information security programme in place that ensures consistent identification and protection of Classified 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 protect will vary from company to company, or even from department to department, but the level of protection should be the same.

Adoption of this scheme will provide current best practice guidance and interoperability on a common approach to appropriate marking and protection of information throughout Herefordshire Partnership Organisations.

12. Interoperability between Organisations

The table below defines the three security (IL) levels matched against the Government and Herefordshire Councils internal classification schemes. Individual Herefordshire Partnership Organisations should use their own terminology to describe these levels and should relate them to their business in terms of the impact or damage, which would arise from unauthorised disclosure. Information identified as IL2 or IL3 should always be marked whether it is on paper, cassette, disk, slide, flip chart, microfiche, photographs or any other media.

All Herefordshire Partnership Organisations can continue to use their own markings but should add the 'ITL' marking at the end, to enable others to recognise the level of classification.

Government Department Classifications	Information Threat level	Herefordshire Council Document Classifications
Restricted	IL3	Restricted
Protect	IL2	Protect
Not Protectively Marked	IL1	Not Protectively Marked

Council Information should not be marked above Restricted.

File	Classification Policy	Pages	13	Version	1.7
Owner	John Pritchard	Distribution	ICT & MRU	Classification	Unclassified

Responsibilities

Everyone is responsible for the information they handle. The Information Security and Data Centre Manager is responsible for updating this document and providing advice on its implementation.

Other Relevant Policies / Council Documents

- Corporate Information Security Policy
- Classification Policy
- Email Usage Policy
- Internet Usage Policy
- Information Security Procedures
- Information Security a Managers Guide
- Information Security Management Manual
- Information Security Response Procedure
- Sharing Internal Data Protocol

Review Date

01/04/2011

Compliance

The information security team and audit services will review compliance of this policy with random spot checks and advice to services.

Impact on the Council's Key Priorities

Without an up to date classification policy we risk harm to people's personal data.

Monitoring Arrangements

All emails sent and received by the Council should be kept for a minimum of 6 months.

Training and Awareness Requirements

All users who have access to information that must go over the Government Secure Intranet (GSI) will be trained in information security before being allowed access to the system. This training will cover classification of documents.

File	Classification Policy	Pages	14	Version	1.7
Owner	John Pritchard	Distribution	ICT & MRU	Classification	Unclassified

Equality Impact Screening Tool

To be completed and attached to any procedural document when submitted to the appropriate committee for consideration and approval.

		Yes/No	Actions
1	Has any base line data been collected on your policy / function and analysed?		(If no then needs to be identified in full impact assessment as this will need to be collected)
2.	Does the policy/guidance affect one group less or more favourably than another on the basis of:		
	Race		If yes, is this justifiable, legal and valid? Give reasons.
	Disability		As above
	Ethnic origins (including travellers)		As above
	Nationality		As above
	Gender		As above
	Culture		As above
	Religion or belief		As above
	Sexual orientation including lesbian, gay and bisexual people		As above
	Age		As above
3	Is it relevant to the general duty under the equality legislation (1. eliminating discrimination 2. promoting equality of opportunity, 3, promoting good relations)	1/2/3	State which it supports.
4	Is the impact of the policy/guidance likely to be negative?		If yes, why and what actions are you going to take?
5.	What alternatives are there to achieving the policy/guidance without the impact?		
6.	Can we reduce the impact by taking different action?		
7.	Is there any public concern that the function and policies are being operated in a discriminatory manner?		
8.	Depending on the above answers does a full impact assessment need to be carried out?		
9.	How is this policy going to be monitored and by whom?		

File	Classification Policy	Pages	15	Version	1.7
Owner	John Pritchard	Distribution	ICT & MRU	Classification	Unclassified

If you have identified a potential discriminatory impact of this procedural document, please refer it to the Corporate Diversity Team who can advise on how to complete a full impact assessment with suggestions as to the action required to avoid/reduce this impact.

Rural Issues Checklist

Each policy should be assessed against two criteria:

- a) does it have a significant or not significant impact on rural communities.
- b) does it have a positive or negative impact on rural communities.

Rural issues are identified below – this list is intended to be a guide not all issues will apply to any one document.

- 1) Protecting/enhancing local facilities and shops
How does the policy affect rural facilities such as village shops, post offices, pubs, garages, other retail outlets, village halls, banks, churches and community enterprises? Can policies be amended to protect or enhance such facilities?
- 2) Maintaining/improving access to services
Does the policy impact on access to and maintenance of services for the rural population, particularly for less mobile groups such as the elderly?
- 3) Improving transport links and options
Will the policy affect transport links and options for commuting, accessing services and recreation? Are different modes and uses of transport considered?
- 4) Tackling poverty and promoting social inclusion
Does the policy affect any disadvantaged groups e.g. elderly, people with disabilities, homeless people, unemployed, women or ethnic minorities? Does it have an impact on sources of information and advice, social services, health, community development and capacity building?
- 5) Providing activities/facilities for young people
Will the policy impact on young people and how?
- 6) Improving employment opportunities
Will the policy impact on employment opportunities and how?
- 7) Strengthening/diversifying the rural economy
Does the policy affect the rural economy? Will it affect market towns, business support, agriculture, manufacturing, tourism, retail, credit sources, community enterprises, farmers markets, training, ICT or start-up premises?

File	Classification Policy	Pages	16	Version	1.7
Owner	John Pritchard	Distribution	ICT & MRU	Classification	Unclassified

8) Provide affordable, quality rural housing

Will the policy affect the affordability and quality of housing across all types of tenure? Does the policy relate to prices, registered social landlords, developers, planning policies, migration, second homes, the elderly or special needs? Does it enhance sustainable communities?

9) Protecting/enhancing the local environment

How does the policy affect the protection and/or enhancing of the local natural and built environment? How sustainable is this?

10) Developing education and training opportunities/facilities

Does the policy impact upon education and training? How does it affect schools, colleges, ICT, access via local facilities or through transport or distance learning?

11) Promoting the use of and access to ICT

Will the policy have an impact on the use of and access to ICT?

12) Encouraging recreation and tourism

Does the policy affect recreation and tourism? Will it have an impact on rights of way, access to the countryside, recreational activities, local heritage, culture, villages and market towns?

If you have identified a potential discriminatory impact of this procedural document, please refer it to the Director of Public Health together with any suggestions as to the action required to avoid/reduce this impact.

File	Classification Policy	Pages	17	Version	1.7
Owner	John Pritchard	Distribution	ICT & MRU	Classification	Unclassified

Environmental (GEM) and Sustainability Checklist

The overarching questions here are

- How will this document impact on our outstanding natural environment?
- Is what is proposed sustainable in the long term?

		Response	Any changes proposed as a result of impacts identified
1	What effect will the document have on carbon/greenhouse gas emissions ¹ ?		
2	How will the operation of the document impact on natural systems? ²		
3	What effect will the document have on the use of resources ³ ?		
4	How would the operation of the document be affected by predictable changes, such as a more unstable climate or increases in the price of oil ⁴ ?		
5	Are there sufficient resources for the provisions set out in the document to be carried out for the foreseeable future?		
6	What effect will the document have on the character of Herefordshire in terms of landscape, buildings, street scene, biodiversity & use of land?		
7	Does the policy enable people to take more responsibility and build their capacity for positive response?		

Please contact the Sustainability Unit if you would like support on either:-

¹ Carbon/GHG emissions result from energy use in buildings, transport & release of other pollutants

² Impacts could include fragmentation or degradation of natural habitat, increased water runoff, potential for pollution, threatening environmental limits

³ Including selection and purchase of materials and costs of disposal

⁴ Climate change is likely to lead to hotter summers and more frequent extreme weather events.

File	Classification Policy	Pages	18	Version	1.7
Owner	John Pritchard	Distribution	ICT & MRU	Classification	Unclassified

- How to assess impacts the document may have or
- How to adjust the document to reduce negative impacts you have identified – or increase positive benefits.

Please send the completed checklist together with the title and brief description of the assessed document to the Sustainability Unit (gem@herefordshire.gov.uk) ahead of the document's final approval.

File	Classification Policy	Pages	19	Version	1.7
Owner	John Pritchard	Distribution	ICT & MRU	Classification	Unclassified