Birmingham City Council

Information Security Labelling and Handling Standard

If you have any inquiries about this Standard,
Contact the Information and Strategy Team (formerly the Business Policy Team, ICF) on 675 1431 or 464 2877

Standard Owner:	Gerry McMullan Information & Strategy Manager, Performance and Information Division, Birmingham City Council
Author:	Mrs M A Westrop – Information Security Manager, Service Birmingham
Version:	4.0
Date:	20/07/2011
Classification	NOT PROTECTIVELY MARKED

Produced in conjunction with SERVICE BIRMINGHAM

CONTENTS

1. OVERVIEW AND PUBLICATION PARTICULARS

Document History

Version Amendment	Date	Purpose	Author
Draft 0.1	23/05/07	Initial Draft	M Westrop
Draft 0.2	14/06/07	Draft after consultation DT&CH of ICF &NJ (see minutes)	M Westrop
Draft 0.3	05/07/07	Draft after documented comments from Reviewers (see detail below)	M Westrop
Draft 0.4	18/07/07	Draft changes after ICF alterations to draft (see ICF document 0.3 reviewed)	M Westrop
Draft 0.5	26/07/07	Changes incorporated after clarification from ICF (see correspondence)	M Westrop
Draft 0.6	02/08/07	In line with 0.6 Code of Practice	M Westrop
Draft 0.7	08/08/07	Corrections after questions put to ICF	M Westrop
Draft 0.8	16/08/07	Update following CISG review	S Tilley / D Thomas
Draft 0.9	30/08/07	Syntax; reinstate capitalised S in Standard.	M Westrop
v1	04/09/07	Update to v1 following BTAG approval	C Hobbs
1.1	12/03/09	Changes for Government GCSx requirements	M Westrop
1.2	08/04/09	Update from review comments	C Hobbs/J Walker
1.3	15/04/09	Amended page breaks and tables & storage paragraph	C Hobbs
1.4	17/04/09	Amended storage paragraph after meeting with SB	C Hobbs
2.0	22/04/09	Approved by BTAG	C Hobbs
2.1	28/05/10	Reviewed and no changes represented to BTAG for comments	D Thomas
3.0	02/06/10	Approved by BTAG	C Hobbs
3.1	03/06/11	Changes to Storage and Transfer in annual review	M Westrop
3.2	16/06/11	Modifications to 3.1 following review particularly incorporating new classification scheme and Council changed to council.	M Westrop
4.0	20/07/11	Approved by BTCG	C Hobbs

Document Distribution after approval

Version	Name	Organisation
1.0	All Staff	Birmingham City Council
2.0	All Staff	Birmingham City Council

Document Reviewers

Version Amendment	Date	Name	Organisation	Role
Draft 0.1, 0.2 & 0.7	260607	Strategy, Policy & Business Security	Service Birmingham	Policy and Security Management
Draft 0.2	260607	Penny Arcatinis	Birmingham City Council	Children's Data Manager
Draft 0.1 & 0.2 – 0.7	260607	ICF	Birmingham City Council	Policy Owners
Draft 0.2	260607	Lynda Bennett	Birmingham City Council	Head of Records Management Service
Draft 0.2	260607	Hadyn Williams	Birmingham City Council	Human Resources
Draft 0.2	260607	Dave Hall	Service Birmingham	City Telecommunications Manager
Draft 0.2	260607	Andrew Mackay	Service Birmingham	Technical Solutions Manager
Draft 0.7	090807	CISG Members	Birmingham City Council& Service Birmingham	

2.1	May 2010	CISG Members	Birmingham City Council & Service Birmingham	

Document Approval by Birmingham City Council

Version	Date	Name	Role
1.0	04/09/2007	BTAG	Approving Body
2.0	22/04/2009	BTAG	Approving Body
3.0	02/06/2010	BTAG	Approving Body
4.0	20/07/2011	BTCG	Approving Body

Overview

Authority[a]	Birmingham City Council – Assistant Director Performance & Information Division
Owner[b]	Birmingham City Council – Information & Strategy Manager
Scope[c]	See introduction below
Review period[d]	This document should be reviewed at least annually or more often if there is change of circumstances.
Related Documents	Information Security Classification Standard; Information Security Policy; Internet Use Policy; Internet Use Code of Practice; Access Control Standard; Disposal of Information Processing Equipment Standard; Information Asset Management; Data Protection Policy; Authentication Security Framework; Records Management Policy; Password Control Standard; Flexible and Remote Access Code of Practice; Ten Email Security Principles for Elected Members; 2008 Security Policy Framework and IA Standard Number 6 within the Manual of Protective Security; Government Connect GSi Code of Connection for GCSx Version 4.1; Information Sharing Protocol – Generic 1.1.
BS ISO/IEC 27001:2005 BS 7799-2:2005 control references	Control Reference A.7 Asset Management A.7.1.1 Inventory of Assets A.7.1.3 Acceptable use of Assets A.7.2 Information Classification A.7.2.2 Information Labelling & Handling A.8.3.3 Removal of Access Rights A.9.1.1.Physical security perimeters A.9.2.1 Equipment siting and protection A.9.2.5 Security of Equipment off-premises A.9.2.6 Secure Disposal or Re-use of equipment A.9.2.7 Removal of Property A.10.1.3 Segregation of Duties A.10.8.1 Information exchange policies and procedures A.10.8.3 Physical media in transit A.11.1.1 Access control policy A.11.2.2 Privilege management A.11.3.2 Unattended user equipment A.11.3.3 Clear desk and clear screen policy A.15 Compliance with legal requirements A 15.1.1 Identification of applicable legislation A.15.1.3 Protection of organizational records.

[a] AUTHORITY: The person or organisation who is responsible for enforcing this Standard.
[b] OWNER: The organisational position of the person who has rights to authorise changes to, or disposal of this Standard
[c] SCOPE: The organisations or persons to whom the Standard applies.
[d] REVIEW PERIOD: How frequently the Standard should be reviewed.

2. PURPOSE OF THE LABELLING AND HANDLING STANDARD

The *Birmingham City Council Information Security Labelling and Handling Standard* contains security rules to protect information controlled by the council, or by a third party on behalf of the council[e]. The council requires all those within the scope of the Standard to follow these rules to protect the confidentiality, integrity and availability of council information.

The handling and labelling rules apply to information classified according to the scheme set out in the *Birmingham City Council Information Security Classification Standard.* This has been changed to fit in with the 2008 Government Security Policy Framework. From April 2009, Birmingham City Council participates in the Secure Government Intranet 'GCSx' network. This means that the council has harmonised its security classifications to cope with information shared between the Government and the council: RESTRICTED, PROTECT and Not Protectively Marked[f].

Scope

This Standard covers all information [g]processed either by the council, or processed on behalf of the council by a third party.

Information may be electronic, graphic, microfiche, film, audio-tape, printed, hand-written, spoken, displayed or stored on any medium.

The obligations outlined in this Standard apply to employees, agency staff, elected members (or other public representatives), trustees, third parties under a contract, employees of associated organisations or volunteers. In addition, those receiving information from Birmingham City Council but who are not part of the council, may have a duty of confidentiality as a matter of law. This Standard applies wherever the work is done, for example at the office, home or a remote site.

[e] In line with ISO 27001:2005 A.7:2:2

[f] See the Information Security Classification Standard available in the PSPG database and on Inline.

[g] Data is processed whenever information is indexed, classified, stored, recorded, disseminated, published, copied, organised, amended, retrieved, viewed, disclosed to others, deleted, destroyed, transferred, transmitted, declassified: *it is difficult to say there is any activity directed towards the data, which does not amount to processing.*

3. STANDARD PARTICULARS

This Standard should be used in conjunction with the *Birmingham City Council Information Security Classification Standard* which sets out three specific Information Security Classifications used by the council: RESTRICTED, PROTECT and Not Protectively Marked.

At all stages in its lifecycle, information should be labelled with its Security Classification and handled with the degree of caution necessary for that Security Classification. Practical advice is set out in the *Birmingham City Council Information Security Labelling and Handling Code of Practice.* **Managers are responsible for deciding the Security Classification of information and the handling procedures in their own business area in line with legislation, financial or audit regulations, Government requirements (including Government Connect[h]) and the particular requirements of their business area.**

Information Lifecycle Summary

Lifecycle stage	**Key principles.** **These are supplemented with practical advice in the** ***Information Security Labelling and Handling Code of Practice.***
Acquisition and Creation	When information is acquired or created, it must be given its Information Security Classification and handled appropriately for that Information Security Classification and any additional particular requirements. Birmingham City Council managers have a responsibility to classify information which must be clearly labelled with its security classification. Files must be marked with the highest security level that has been given to any item of information within that file.
Storage	When anyone stores information on any council equipment[i] the stored information must be relevant to their duties and this must only be done in the course of those duties. This restriction does not apply to information temporarily stored as a result of personal use of email or the Internet. The council reserves the right to monitor and investigate any information stored on its systems. All information files must be labelled with the highest level of security classification required within the file. Handling rules for each classification are described in the *Information Security Labelling and Handling Code of Practice*.

[h] Government Connect is a network between central government and every local authority in England and Wales, known as GCSx (Government Connect Secure Extranet).

[i] This includes personal and shared network drives and local hard drives

Lifecycle stage	Key principles. These are supplemented with practical advice in the *Information Security Labelling and Handling Code of Practice.*
Access	Access rights to information (manual or computer information systems) should be role-based and not individually-based: that means that a particular individual can access RESTRICTED or PROTECT information in the course of their work only if their job or role within the council justifies this. See the council's *Access Control Standard* for further guidance. Access to information classified as RESTRICTED and PROTECT, (which will include all sensitive personal information), must be limited to those authorised to view it. RESTRICTED or PROTECT information must always be safeguarded by authentication formalities, whatever storage system is used[j]. Information shared through the GCSx Government Connect network must be Processed only on equipment owned by the council and connected to the council's networks directly[k] and kept on council-controlled premises. Other information, (but never information available to GCSx), may be processed remotely as set out in the *Flexible and Remote Access Standard.*
Prints, copies or other portable media	Portable information may be held on paper (for example, prints and copies) or other non-digital media or portable electronic memory (for example, CDs and memory sticks). It must be labelled with its Security Classification. Access to portable information must be restricted solely to relevant people and information must be stored securely in order to prevent unauthorised access. Files must be marked with the highest security level that has been given to any item of information in that file. All portable use of RESTRICTED information should be recorded in an audit log[l]. Unless it is deliberately reassessed and re-classified, portable information inherits the same Information Security Classification as the original from which it was copied. Portable information should be appropriately labelled with its Information Security Classification. Information released under the Freedom of Information Act must be classified as Not Protectively Marked. It is the responsibility of the person using copied or portable data to keep it securely. It is a manager's responsibility in their business area to decide what portable handling needs to be specifically authorised.

[j] Authentication formalities are the procedures used to verify the identity of the person using the information and record and limit their access to the information: for example, the person who gains access must have a unique identity and secret password; they must be formally authorized and granted an identity before they gain access; they should have access levels appropriate for their job duties, etc. Full controls are set out in ISO27001.

[k] Direct connections do not pass through the internet or networks not owned and managed by the council. For example, Blackberry connections to GCSx data are not permitted.

[l] An audit log template is available on the PSPG database.

Lifecycle stage	Key principles. These are supplemented with practical advice in the *Information Security Labelling and Handling Code of Practice.*
Retention, Back Up, Archiving and Destruction	When mobile devices and portable memory devices are due to be de-commissioned, the person responsible for the information on those devices must consider if the information should be retained, archived or destroyed. Information which is due to be destroyed is always classified as RESTRICTED. Refer to your Directorate's retention schedules and the *Records Management Policy* for advice about whether the information should be retained, destroyed or archived.
Transfer and Exchange of Information	It is presumed that all information which not protectively marked will be available to the public under Freedom of Information rules, unless there is a legal obligation not to exchange this information. Protectively marked Information should not be exchanged or transferred unless there is clear justification and authorisation. When information is exchanged with parties outside the council, it is the sender's responsibility to comply with all legislative and contractual obligations. The sender must be satisfied that the recipient is properly identified and authorised to receive the information. There are restrictions on methods of transfer set out in the *Labelling and Handling Code of Practice*. The recipient of the information must be made aware of any duty of confidentiality and other contractual obligations required by Birmingham City Council when the information is sent[m]. The sender must always label transferred or exchanged information with the appropriate label: RESTRICTED, PROTECT or Not Protectively Marked. When anyone in the scope of this Standard transmits digital RESTRICTED or PROTECT information, **two-levels of security** are required: see the *Handling and Labelling Code of Practice*. Information released under the Freedom of Information Act must be classified as Not Protectively Marked. Information within the GCSx network must not be transferred to any equipment or network owned by third parties.

[m] In line with ISO27001:2005 A 10.8.1

4. ROLES AND RESPONSIBILITIES

Role	Organisation	Responsibility
Employees, agency staff, elected members or other public representatives, trustees, third parties under a contract, employees of associated organisations or volunteers	All within Scope	To comply with this *Standard* & related documents.
Corporate Management Team	Birmingham City Council	To manage and maintain controls which limit access to information as required in this Standard.
Intelligent Client Function – Business Policy Manager	Birmingham City Council	To make sure the *Information Security Labelling and Handling Standard* meets business needs and is reviewed annually as a minimum; To make managers aware of the requirements of the GCSx Code of Connection.
Birmingham City Council Managers	Birmingham City Council; Service Birmingham on behalf of Birmingham City Council.	To manage information labelling and handling locally within the organisation and to decide the appropriate information security classification for each database; To provide suitable training about the security Standards and Policies and to communicate this *Standard* and the *Code of Practice* to Staff; To make third party organisations aware that the council's *Information Security Labelling and Handling Standard* is the minimum requirement when information is exchanged; To communicate issues and anomalies back to the Corporate Management Team. To understand and follow the requirements of the GCSx code of connection when dealing with Government Connect information.
Head of Records Management Service	Birmingham City Council	To advise on records management within the council.

5. EXCEPTIONS

There are no exceptions to this Standard.

6. ENFORCEMENT

Any member of staff who contravenes this Standard may be investigated under the council's disciplinary procedure and, where appropriate, legal action will be taken.

Third parties, partners and other individuals within the scope[n] of this Standard, who contravene its terms, may have their right to handle council information revoked and may jeopardise their relationship with Birmingham City Council. They may also face legal action.

[n] See Scope, above.

[n] In line with ISO27001:2005 A 10.8.1