# Birmingham City Council

# Information Security Classification Standard

If you have enquiries about this Standard,
contact the Intelligent Client Function on 0121 675 1431 or 0121 464 2877.


| | |
|---|---|
| Standard Owner: | Gerry McMullan – Information and Strategy Manager, Birmingham City Council |
| Author: | Jill Walker – Manager – Security, Service Birmingham |


| | |
|---|---|
| Version: | 8.0 |
| Date: | 24 May 2012 |
| Classification: | NOT PROTECTIVELY MARKED |



Produced in conjunction with

CONTENTS

## 1. PURPOSE OF THE STANDARD

This standard defines how information should be classified in order to achieve an appropriate level of protection.

Classification should be assigned according to the degree of harm that would be caused if the information were compromised. The guidelines contained in this Standard conform to the HM Government (HMG) Security Policy Framework (SPF).

The SPF sets out some minimum standards for information security which must be adopted by agencies working with Central Government, including Local Government. Birmingham City Council (BCC) participates in the Secure Government Intranet 'GCSx' network which complies with the SPF. This means that BCC must apply relevant parts of the protective marking system prescribed in Security Policy No 2 contained within the SPF to information shared between the Government and the City Council; as well as to information released under the Freedom of Information Act (FOI) and to personal data and data released under the Data Protection Act (DPA) and other legislation.

## 2. SCOPE

This Standard covers all information processed[a] either by BCC, or processed on behalf of BCC 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 but who are not part of BCC, may have a duty of confidentiality. This Standard applies wherever the work is done, for example at the office, home or a remote site.

## 3. CLASSIFICATION STANDARD

Information is controlled in the various business units within BCC and managers have responsibility for classification of this information which must be clearly marked with its security classification.

The public is able to access a large proportion of BCC information under the FOI Act 2000, DPA 1998 and other legislation, subject to a number of exemptions. The information made available to the public is marked NOT PROTECTIVELY MARKED and information that is not visibly classified will be assumed to be thus.

[a] 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.*

Information must be protected throughout its lifecycle from creation to its authorised disposal. In keeping with its security classification, information should be kept securely and its accuracy must be maintained; it must be available for authorised use or disclosure when required. Rules for labelling and handling information are set out in the *Labelling and Handling Standard*[b] and *Code of Practice*[b] and related documents.

[b] For policy details, look on Inline, in the PSPG Database or contact the Intelligent Client Function on 5/1431 or 4/2877.

## 4. ROLES AND RESPONSIBILITIES

| Role | Responsibility |
|---|---|
| Corporate Management Team | For the management of BCC's information assets. |
| Information and Strategy Manager | To keep the Information Security Classification Standard relevant to business needs and is reviewed at least annually. |
| Managers of teams that handle records, files or other forms of information | To manage information assets at a local level and keep them securely;<br><br>To classify information appropriately and periodically to review the security classification;<br><br>To review access rights associated with the information in order to ensure they are current and valid;<br><br>To put security controls in place which are appropriate to the information's security classification;<br><br>To give third parties and external agencies access only to information to which they are authorised and to make them aware of the BCC Information Classification Standard and associated handling procedures when information is shared;<br><br>To give consideration to the interpretation of Security Classification of documents from other organisations.<br><br>To restrict access for third parties and external agencies working in partnership with BCC only to information for which they have authorised access. |
| BCC | To communicate BCC's Information Classification Standard and associated handling procedures to their staff. |
| Staff (Permanent, temporary, casual and seconded employees) and Elected Members | To access only information which they are authorised to access.<br><br>To process BCC information in line with its Policies. |

## NS

eptions to this Standard.

## MENT

ember of staff found contravening this standard or jeopardising the security of s the property of BCC may be investigated under BCC's disciplinary procedure priate, legal action may be taken.

artner organisations found contravening this standard or jeopardising the ation that is the property of BCC may be investigated and, where appropriate, be taken.

## ON PARTICULARS

| Date | Purpose | Author |
|---|---|---|
| 22/04/09 | Approved by BTAG | C Hobbs |
| 18/03/10 | Draft for comments from CISG | J Walker |
| 25/03/10 | Forwarded to BPT for sign off at BTAG | J Walker |
| 19/04/10 | Approved by BTAG | C Hobbs |
| 15/02/11 | Annual review | J Walker |
| 04/04/11 | Amendments following review comments | J Walker |
| 18/05/11 | Approved by BTCG | C Hobbs |
| 26/04/12 | Draft for comments from CISG | J Walker |
| 15/05/12 | Forwarded to I&S for sign off at BTCG | J Walker |

Overview

| | |
|---|---|
| Authority[c] | Birmingham City Council – Head of Policy & Co-ordination |
| Owner[d] | Birmingham City Council – Business Policy Manager |
| Scope[e] | All information held and/or processed by BCC; or on behalf of BCC by a Third Party. |
| Review period[f] | This document will be reviewed annually as a minimum or more often if there is a change of influencing circumstances. |
| Related documents | BCC Information Security Policy<br>BCC Labelling & Handling Standard<br>BCC Disposal of Information Processing Standard<br>The HMG Security Policy Framework (SPF)<br>Government Connect GSi Code of Connection (GCSx Versions 3.2 and 4.1)<br>GCSx Acceptable use standard and Personal Commitment statement |
| BS ISO/IEC 27001:2005<br><br>BS 7799-2:2005<br><br>control references | Control Reference<br>A.7 Asset Management<br>A.7.1.1 Inventory of Assets<br>A.7.1.2 Ownership of Assets<br>A.7.1.3 Acceptable use of Assets<br>A.7.2 Information Classification<br>A.7.2.1 Classification Guidelines<br>A.7.2.2 Information Labelling & Handling<br>A.8.3.2 Return of Assets<br>A.8.3.3 Removal of Access Rights<br>A.9.2.6 Secure Disposal or Re-use of equipment<br>A.9.2.7 Removal of Property<br>A.10.1.3 Segregation of Duties |

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