1. OVERVIEW AND PUBLICATION PARTICULARS

Document History

Version	Date	Purpose

Overview

Authority[a]	Birmingham City Council – Head of Policy & Co-ordination
Owner[b]	Birmingham City Council – Business Policy 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 Birmingham City Council 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 Sharing Protocol; 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; the 2008 Security Policy Framework and IA Standard Number 6 within the Manual of Protective Security; *Information Loss Standard* and the *Information Security Incident Response Standard.* Government Connect GSi Code of Connection for GCSx Version 4.1
BS ISO/IEC 27001:2005 BS 7799-2:2005	

2. PURPOSE OF THE LABELLING AND HANDLING CODE OF PRACTICE

The Birmingham City Council Labelling and Handling Code of Practice contain rules for everyone who handles information for the council, that is to say everyone within the scope of the *Birmingham City Council Labelling and Handling Standard*[e] and the Government Connect Secure Extranet (GCSx) Code of Connection requirements[f].

Those who are within the scope of the Standard must follow the advice in order to keep the council's information securely and comply with that Standard.

3. What is Processed Information?

Information or 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.*

4. CODE OF PRACTICE

Labelling and Handling Requirements for All Information

All information must be conspicuously labelled with its Security Classification[g].

Birmingham City Council managers are responsible for making sure all information is labelled with its Security Classification. Files must be marked with the highest security level that has been given to any item of information in that file. Information that is not specifically labelled will be considered to have a classification of "Not Protectively Marked".

Most information handled by the council is classified as "PROTECT" and is available only to a controlled number of people. More sensitive or valuable information might be classified as "RESTRICTED". Three categories are set out in the *Information Security Classification Standard* and readers should read this in conjunction with the Labelling and Handling advice.

[e] See the section on 'Scope' within the *Labelling and Handling Standard*.
[f] The Secure Government network GCSx: see the *Labelling and Handling Standard*.
[g] All Standards and Codes of Practice are available in PSPG database and on Inline.

ACQUISITION AND CREATION

When information is acquired or created, it must be given its Security Classification and handled appropriately for that Security Classification and additional particular requirements[h]. In every area of the council, it is the responsibility of all managers for that area to see to this.

Many particular requirements exist under the law, council standards and policies. For example, there are important requirements set out in the Data Protection Act; the *Birmingham City Council Internet Monitoring Standard* and the *Email Use Policy*. Managers must make themselves and their teams familiar with all the particular requirements of their own business areas.

Investigations have their own rules and evidential requirements. For more details about how evidence should be acquired, see the Investigation Access page in Inline[i] or contact Internal Audit.

STORAGE

All information used to conduct the council's business must be recorded in a filing system: this applies to all media, whether it is electronic, paper, photographs or other. All filing systems should have a

1. Security Classification based on the *Information Security Classification Standard*,
2. retention schedule and
3. data protection registration where personal data is contained in the database.

Managers are jointly and individually responsible for deciding and agreeing the Security Classifications and retention dates in their own business area[j]. Records Management Service[k] can help here.

Information must be stored appropriately for its Security Classification. For example, paper information classified as "PROTECT" or "RESTRICTED", should be locked away in cupboards. See the notes on physical security, below.

Storage of Information not owned by the Council

When anyone stores information on any council equipment[l], this must only be done in the course of authorised work for the council. For example, those who use the council's equipment may not store on any council computer drive copyrighted films or music which they have acquired for a purpose not connected with Birmingham City Council authorised work.

This restriction does not apply to information automatically stored by the system without the intervention of any user, as a result of permitted personal use of email or the Internet. The

[h] See the City Council's *Information Labelling and Handling Standard*

[i] Investigation access details are available on Inline, the City Council's intranet.

[j] Managers should follow the Council's Information Security Classification Standard and Retention Period Schedule

[k] 303 2498 at Nov 2010. Records management can carry out surveys to identify what records are held by a specific business area and can then produce retention schedules for the area concerned. Their service is, however, a limited one and some of it is chargeable.

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

council reserves the right to monitor and investigate any information stored on its systems, including information stored as a result of personal use of email or the Internet. The council also reserves the right to discard any information stored on council equipment as a result of personal use of the council's systems.

When third party-owned personal information is stored on the council's equipment merely in order to facilitate the transfer information onto third party equipment, the party who provides that information will be responsible for its security unless there is an express provision otherwise. For example, if a home worker stores their private home email address on a council owned laptop, in order to send work home, the council is not responsible for the subsequent loss or misuse of that email address, except by express contractual provision.

ACCESS[o]

Access to council business information should be role-based and not individually-based[p]: this means that a person can access information classified as “RESTRICTED” or “PROTECT”,   in the course of their work, only if their job or role within the council justifies this. Information should not be kept where only one individual can access it[q].

GCSx information

A note on Passwords and Password Protect Codes

The *Birmingham City Council Password Policy* and the Inline advice pages set out rules which include the important principle that passwords should never be shared .

Note that this applies to individual passwords you use when you log onto systems or equipment. There is a separate and unrelated Password Protect Code, which you can apply to documents separated from systems (email attachments; separately stored Microsoft Word or Excel documents, for example). These password protect codes must be shared so that, if one person is unavailable to open the file, others can do this. Passwords for password protected documents should be restricted to a list of authorized personnel, which is maintained within office procedures documentation, and which allows for passwords to be changed when necessary.

Access to non-system information - portable prints, copies and portable data generally [t] - three principles.

Portable information is contained in hard copy (paper, photographs, microfiche, maps etc) or on portable media (for example memory sticks, CD’s, laptops, mobile telephones, Blackberries, palm held devices, cameras etc.). Access to portable information will not usually be audited or authenticated automatically, and therefore it is important to label, authorise, and maintain the audit trail.

1. Labelling

Portable information must be labelled with its security classification, and possibly with extra labels such as “personal” or “confidential”.

If “RESTRICTED” information is converted to any portable format and removed from the workplace for any reason, (for example, printed out and taken to an external meeting), there should be one person who agrees to take custody and responsibility for looking after it safely. If nobody takes responsibility by agreement, then the handler who printed it, is responsible. If you are handing “RESTRICTED” information to someone else who then becomes responsible for it, make them sign a receipt for it and keep the receipt as part of an audit log or you remain responsible.

See also the rules on transferring information and the single point of contact (“SPOC”) (Information transfer between organisations, below).

3. Audit log

All portable use of RESTRICTED information should be recorded in an audit log[u]. See also the notes on physical security below.

USE

Information must be used in compliance with council policy and statute and with the agreed Government GCSx Code of Connection. Of particular importance is the Data Protection Act, which contains rules about handling personal information.

Rules for the Physical security of informa tion classified “PROTECT” or “RESTRICTED”.

1. When you discuss information classified “PROTECT”, “Confidential” or “RESTRICTED”, in
.

DESTRUCTION

Information no longer required and of no archive value, must be destroyed. All information which is no longer required, and should be destroyed, is classified as RESTRICTED to stop its being inadvertently used. This is dealt with in three separate areas of policy[dd]:

Removable Media
The *Records Management Policy* details the rules for the disposal of paper and microfilm records, as well as removable storage devices such as memory sticks, CDs and floppy disks – but not telephones. See the Records Management pages on Inline for more

Electronic transfer, of “RESTRICTED” information should always be done through two level security .

Two level security for information Processed remotely

RESTRICTED information should always be protected by authentication formalities. Whenever it is viewed remotely it should ideally be protected by an additional security barrier. The first security level is usually provided by the fact that to access the data, a data user (sending or receiving) must enter a password and user identity – as they would if the data was accessed locally rather than remotely. The second level of security is ideally achieved by the additional use of encryption.

For example, a Virtual Private Network connection can be set up so that a worker can view their computer terminal from home using internet connections to make their terminal at home appear as if it is the computer at work, At connection, the user will be required to enter a password, user identity and the data that travels to and from the home from Birmingham City Council will be encrypted. These safeguards – password and encryption - comprise the two levels of security necessary.

Additional security is also an option. Equipment or software which only allows access when the user passes another security barrier may be needed. The user might, for example, set up a Personal Identification Number code or have a security fob, which they use to unlock the software and hardware where they are processing the information. These measures should be weighed up, along with the costs and risks involved[hh].

World Wide Web File Transfers

There are specific rules about what you can, and cannot, transfer through a Birmingham City Council internet account: see the council’s *Internet Use Policy* and *Internet Use Code of Practice*.

If you transfer files through the world wide web and if, furthermore, this is not to an organisation connected to GCSx, you should ask the Service Desk to set up secure file transfer protocol (“SFTP”) through the City’s firewall.

RESTRICTED Information transfer – see also access to portable information, above .

Some RESTRICTED and sensitive personal information extracts may have to be carried around by council staff in order to carry out council business in remote locations. The business areas concerned should document the procedure and should consult Strategy, Policy and Business Security about what precautions are necessary. The user must develop formalities and logs[ii] to show when information is taken in and when it is returned or destroyed, and by whom. Documents not returned or destroyed must be periodically chased up and counted.

The person with custody of the information must additionally, take responsibility for information security lapses (see notes on portable information access, above). (If the transfer is between organisations, the SPOC will also be responsible).

[hh] If you want technical advice about this, contact the Service Birmingham Service Desk on 464 4444. This service may be chargeable.

[ii] See the template audit log on the PSPG database

For example, Sensitive RESTRICTED information for child protection may be needed by child protection courts. These extracts should be labelled, used and then returned or destroyed in a way approved by business security, and this process should be tracked in an audit log,

In general, before information is transferred to other organisations or individuals, the sender must be satisfied that this is an appropriate recipient and that they are made aware of any duty of confidentiality required by Birmingham City Council when they send this information.

The sender must also be satisfied that the recipient has the required security clearance whenever they transfer information

GUIDE TO VARIOUS METHODS OF INFORMATION TRANSFER: MAIL, FAX, &c for non-GCSx data

U = do not use this method V= permitted with precautions

Transmission Method	RESTRICTED	PROTECT	NOT PROTECTIVELY MARKED
By hand	V (with signed receipt for audit log)	V	V
By internal mail within the same building	U	V	V
By standard post	U	V Label the outside of the envelope “Confidential” if appropriate and make sure the envelope is opaque and not one with a window. There should always be a named individual recipient.	V
By recorded/special delivery or courier[kk] Always use “tracking” services and arrange for parcels to be delivered with receipt signatures only.	V Not recommended . Note other guidelines for RESTRICTED or Confidential information. Label the outside of “To be opened only by the addressee” and log the transfer.	V Also note that there are Data Protection restrictions on sending personal information outside the country. Label the outside of the envelope “Confidential” if appropriate and make sure the envelope is opaque.	V
By facsimile The recipient should be contacted to confirm they are on stand by and again to confirm they have received the communication. Label the cover sheet “Confidential” if appropriate.	NO U	V Note that there are Data Protection restrictions when personal data is sent abroad. The recipient should be contacted to confirm they are on stand-by and again to confirm they have received the communication.	
By email Label the subject header Confidential and/or RESTRICTED as appropriate.	V NB electronic transmission of RESTRICTED information needs two levels of security; always log the transfer for an audit trail.	V Note that there are Data Protection restrictions when personal data is sent abroad.	
By telephone	V Use equipment approved by Service Birmingham and do not use speakerphone and don’t leave information on answer phone. Information should be kept out of earshot of unauthorized personnel.		V

[kk] There is no approved list of couriers. Use 'contracted suppliers' where there is already a corporate or local contract. Contact Corporate Procurement Services on 3-0303 to find out what contracts are already in place. If there is no existing contract, it is best practice to get three quotations and record why a particular firm is chosen.