



Birmingham City Council

Loss of Information or Equipment Containing Information Standard

If you have enquiries about this Standard,
Contact the Information and Strategy Team on 0121 675 1431 or 0121 464 2877.

Standard Owner: Gerry McMullan, Information and Strategy Manager
Birmingham City Council

Authors: Jill Walker – Manager – Security
Service Birmingham

Version: 6.0

Date: 01/03/2012

Classification NOT PROTECTIVELY MARKED

© Birmingham City Council 2012



Produced in conjunction with

CONTENTS

PURPOSE OF THE STANDARD	3
1. SECURITY RISKS CONSIDERATIONS.....	3
2. ROLES AND RESPONSIBILITIES	5
3. EXCEPTIONS.....	8
4. ENFORCEMENT	8
5. DEFINITIONS	9
6. OVERVIEW AND PUBLICATION PARTICULARS.....	10

PURPOSE OF THE STANDARD

The purpose of this Standard is to set out the procedure and considerations for reporting and handling the loss of information held by, or processed on behalf of, Birmingham City Council.

The Standard is particularly concerned with the loss of personal data, and is designed to operate in conjunction with the council's standards pertaining to personal data and information security.

Scope

This Standard applies to all information processed by Birmingham City Council, or processed on behalf of the council by a third party. Loss of information includes the loss of all equipment containing such information.

Loss of information includes actual or suspected theft and/or accidental loss or destruction and/or unauthorised disclosure.

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 anyone handling council information including employees, agency staff, elected members (or other public representatives), trustees, third parties under a contract, employees of associated organisations or volunteers. This Standard applies wherever the information is processed, for example at the office, in transit, at home or at a remote site.

1. SECURITY RISKS CONSIDERATIONS

Information loss and Data Protection Act breaches have now become much more newsworthy and as a result, the public are increasingly aware and concerned about loss of their personal data.

Technological Risks

Council policy requires the use of additional security whenever information classified as PROTECT or RESTRICTED¹, such as personal data², is transferred or processed remotely. The preferred security arrangement is to use encryption. Personal or sensitive data must not be held on a memory stick unless it is absolutely unavoidable. If it is unavoidable then the information must be encrypted.

Compliance and Legal Risks

The Information Commissioner has been granted stronger powers³ which allow him to fine Data Controllers⁴ where there is evidence that the data protection principles as defined in the Data Protection Act 1998 have been contravened, and this contravention is likely to cause substantial damage or substantial distress to the Data Subject⁵. Breaches can occur either as a result of Birmingham City Council's own fault, or because of the behaviour of a contractor or partner organisation. In either case, the Data Controller, Birmingham City Council, is responsible⁶.

¹ See the Information Security Classification Standard available in the PSPG database on Lotus Notes

² Labelling and Handling Code of Practice available in the PSPG database on Lotus Notes

³ Criminal Justice and Immigration Act 2008.

⁴ Person (i.e. natural person or legal body such as a business or public authority (Birmingham City Council) who decides the manner in which, and purpose for which, personal data is processed.

⁵ An individual who is the subject of the personal data/information.

⁶ The information Commissioner made its first Data Protection Act fines in November 2010. Hertfordshire County Council was fined £100,000 for sending 2 separate faxes in June 2010 containing personal sensitive information to the wrong recipients. Sheffield-based A4e was fined £60,000 for losing an unencrypted laptop in June 2010 containing the details of thousands of people. The maximum fine that the Information Commissioner can impose is £500,000.

Various other obligations, such as the provisions of Government Connect (GCSx), impose the requirement to have a process to report and investigate security incidents. Local Authorities are obliged to report certain breaches of the Government Connect Code of Connection through the national information security incident reporting arrangements, including the regional WARPs. The Government and the Information Commissioner have powers to prosecute individuals for breach of the Data Protection Act, in certain cases.

Information Security

Birmingham City Council and Service Birmingham are working towards compliance with the international standard in Information Security, ISO27001. This requires that security incidents and weaknesses should be reported as quickly as possible. See the Information Security Incident Response Standard which can be found in the PSPG database on Lotus Notes for the process to be followed.

STANDARD PARTICULARS

Anyone discovering a loss or suspecting a breach must report the loss, theft or wrongful disclosure of council information to the Information and Strategy Team, Performance and Information Division, Corporate Resources Directorate either by telephone on (675 1431/464 2877) or via Lotus Notes to the Information and Strategy Team Mailbox, within one day of discovering or first suspecting the loss.

Notification can come from anywhere – for example, from council staff, senior management, CISG Representatives, Service Birmingham, managers of external contractors, or from the Information and Strategy Team. All loss of information or equipment, including breaches by external contractors, must be handled in the same way. Standard terms must be included in all contracts stipulating an obligation for a contractor to notify the council within one working day of the contractor being made aware or suspecting that a breach has occurred.

The Information and Strategy Team will record any incident reported on a data loss register⁷. A case number will be assigned and the Information and Strategy Team will send out a questionnaire within one working day. The responses received in the questionnaire will be assessed within one working day of receipt. Advice on any other action to be taken will also be given e.g. reporting loss of equipment to the police and the Service Birmingham Service Desk; advising the press office etc.

In suspected cases of personal data loss, the Information and Strategy Team will forward a copy of the completed questionnaire and a Personal Data Security Breach Notification Form to the directorate CISG representative⁸ for their completion. The CISG representative must inform an appropriate Assistant Director of the loss. The Personal Data Security Breach Notification Form holds the following information:

- When the incident occurred
- A brief description of the incident
- How many data subjects have been affected
- Whether the data subjects have been notified
- If there has been any media coverage of the incident
- Any action taken to mitigate the effect on the data subjects involved
- Details of the directorate investigation into the incident
- Details of any other regulatory bodies that have been informed of the incident
- Details of any actions taken to prevent similar incidents in the future

⁷ In particular, information, where available, will be useful if it is about the Information Security Classification, sensitivity and quantity of any data lost or compromised; whether and how much personal data was lost or compromised; the type of equipment lost (laptop, CD, memory stick, letter etc); the value of the data or equipment lost, whether it was encrypted; the application containing the lost data; the owner of the data; the name of the person responsible for the data when it was compromised and his/her directorate and line manager.

⁸ A current list of CISG representatives can be found on Inline.

- Any other information that would be helpful in assessing the incident.

Other information losses that are judged to be significant⁹ will be reported by the Information and Strategy Team to the Directorate CISG representative which may result in Legal Services, Birmingham Audit and an Assistant Director of the Directorate getting involved. The Assistant Director will appoint an investigating officer from the Directorate to handle the investigation. The Director can elect, depending on the severity and impact of the breach or loss, to inform the Chief Executive and the Leader and Deputy Leader.

Where necessary the Information and Strategy Team will inform the relevant Service Birmingham Teams who will arrange for the blocking of any equipment and accounts - User ID's and communication accounts (for example, 3G telephone connection accounts which allow laptops to connect with Birmingham City Council equipment remotely) may be disabled if it is suspected that they have been compromised. The Information and Strategy Team will also check, in the case of lost or stolen equipment, that Credant Data Encryption Software was installed.

The Directorate Investigating Officer is responsible for effecting the right level of response, for coordinating any measures to assess risk and mitigate the loss, with assistance from the Information and Strategy Team, Legal Services and Birmingham Audit as required. This may involve contacting the Information Commissioner's office, the police, the council's press office, the Corporate Information Management Team or any other team or individual affected by the loss. Action must be taken promptly:

1. to minimise any detrimental impact to the data subjects arising from any loss or breach;
2. to contain and prevent any further damage from the existing loss or breach;
3. to liaise with the Information Commissioner and other external regulatory bodies where appropriate;
4. to minimise any detrimental impact on the council both in terms of damage to the council's reputation but more importantly protecting the interests of both the citizens and the council's staff
5. undertake any actions identified in consultation with Legal Services, Birmingham Audit and the Information and Strategy Team.

An initial meeting can be called by the Investigating Officer, if the loss or breach is deemed of a serious nature, to discuss the actions to be taken.

After a breach has been dealt with a post mortem meeting will be arranged with representatives from all parties that have been involved to ascertain the cause of the loss or breach, and to advise the council about preventing re-occurrences of the loss or breach.

This cross-directorate group would normally comprise representatives from Legal Services, Information and Strategy Team, Corporate Information Management Team, a senior representative of (each of) the Directorate(s) involved, CISG rep(s) for the Directorate(s) involved, Birmingham Audit and where necessary, SP&BS, Link2ICT (for schools losses), a representative of any third party contractor involved and Communications Team(s).

2. ROLES AND RESPONSIBILITIES

Role	Responsibilities
Birmingham City Council Corporate Management Team	<ul style="list-style-type: none"> • to ensure implementation of this Standard across the council • to receive communication about data loss incidents as appropriate

⁹ Significant in this instance describes information losses that would spark media interest, be of interest for commercial purposes, are politically sensitive and/or contain details that would allow the finder to steal money or commit fraud, eg, credit card details.

<p>Birmingham City Council Information and Strategy Team</p>	<ul style="list-style-type: none"> • to be the first point of contact for reporting lost data whether in paper or electronic format • to record the loss in the Data Loss Register and allocate a case number • to issue the data loss questionnaire and collate the response • to perform an initial assessment of the significance of the loss • if the loss is significant the team will inform the Directorate CISG representative by sending a copy of the completed questionnaire and a Personal Information Security Breach Notification Form. The team will also inform Service Birmingham Teams (if required) in order to request the blocking of IDs and communication accounts as necessary, Legal Services and Birmingham Audit of the loss by e-mail (if the loss is judged significant). • to advise the individual of any other immediate action required – e.g. report loss of equipment to the police • to track progress of any investigation undertaken • to arrange and attend the post mortem meeting.
<p>Role</p>	<p>Responsibilities</p>
<p>Service Birmingham Strategy, Policy and Business Security Team (SP&BS)</p>	<ul style="list-style-type: none"> • to report any data and/or equipment loss reports received to the Information and Strategy Team. • to advise on security issues as requested by the Information and Strategy Team. • to attend the post mortem meeting as required.
<p>Service Birmingham Service Desk</p>	<ul style="list-style-type: none"> • to log calls regarding data and/or equipment loss.
<p>Assistant Director (or Head Teacher/Chair of Governors if event relates to a school).</p>	<ul style="list-style-type: none"> • to assume responsibility for any data loss or breach in their directorate/establishment • to appoint and brief an Investigating Officer • notify the Chief Executive and the Leader/Deputy Leader as appropriate • notify the Information Commissioner's Office and other affected parties as appropriate.
<p>Directorate Investigating Officer</p>	<ul style="list-style-type: none"> • to investigate the loss or breach within their Directorate • to undertake any actions identified in consultation with Legal Services, Birmingham Audit and the Information and Strategy Team • to return completed Personal Data Security Breach Notification Form to the Information and Strategy Team

	<ul style="list-style-type: none"> to advise management regarding actions to be taken (including any disciplinary action) to attend the post mortem meeting.
Corporate Information Security Group (CISG) representative	<ul style="list-style-type: none"> to advise the Assistant Director and Investigating Officer as required to undertake any actions as required by the Information and Strategy Team or the Assistant Director to attend post mortem meeting for any loss or breach in their Directorate.
Birmingham Audit	<ul style="list-style-type: none"> to receive notification of significant data loss and breach events to provide advice and guidance as appropriate to conduct risk assessments on losses or breaches as appropriate to ensure all standard contract terms with third parties allow Audit to conduct investigations in relation to breaches and losses where such events have occurred by contractors / data processors acting on behalf of Birmingham City Council to attend the post mortem meeting.
Birmingham City Council Legal Services	<ul style="list-style-type: none"> to receive notification of all significant data losses to provide advice and guidance as appropriate to attend the post mortem meeting.
Role	Responsibilities
Corporate Procurement	<ul style="list-style-type: none"> to ensure all standard contract terms stipulate an obligation for a contractor to notify the council within one working day of the contractor being made aware or suspecting that a breach or data loss has occurred. to ensure all standard contract terms with third parties allow Audit to conduct investigations in relation to breaches and losses where such events have occurred by contractors / data processors acting on behalf of Birmingham City Council
Birmingham City Council staff (permanent, temporary, casual and seconded employees) and elected members	<ul style="list-style-type: none"> to ensure that they are aware of the procedure for reporting loss of equipment and information to report any loss of information or equipment containing information to the Information and Strategy Team within one day of the loss.
Birmingham City Council Corporate	<ul style="list-style-type: none"> to provide advice and guidance as required

Communications/Press Office	<ul style="list-style-type: none">• to handle any enquiries from the press regarding data loss or breach.
Third Party Contractor	<ul style="list-style-type: none">• to participate in investigations where breach or loss is their responsibility.

3. EXCEPTIONS

There are no exceptions to this Standard.

4. ENFORCEMENT

Any individual member of staff who contravenes this Standard or jeopardises the security of the council's information is liable to disciplinary action under the council's disciplinary procedure and, where appropriate, legal action may be taken.

Third parties or partner organisations which contravene this Standard or jeopardise the security of the council's information will liable to be investigated and, where appropriate, legal action may be taken.

5. DEFINITIONS

DPA	means the Data Protection Act 1998.
ICO	means the Information Commissioner's Office, the statutory regulator responsible for enforcing the Data Protection Act.
Breach	means the actual or suspected loss or unauthorised access and/or disclosure of information held by, or on behalf of, Birmingham City Council.
Process	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: <i>it is difficult to say there is any activity directed towards the data, which does not amount to processing.</i>
CISG	Birmingham City Council Corporate Information Security Group.
SP&BS	Strategy, Policy and Business Security Team, Service Birmingham.
GCSx	Government Connect Secure Extranet (GCSx) is a private Wide-Area Network (WAN) which enables secure interactions between connected Local Authorities and organisations. Certain members of staff in the council are required to use the applications operated on this network in order to carry out their roles on behalf of the council. These applications include secure e-mail accounts.
WARP	Warning Advice and Reporting Point

6. OVERVIEW AND PUBLICATION PARTICULARS

Authority ¹⁰	Birmingham City Council – Assistant Director – Performance and Information Division
Owner ¹¹	Birmingham City Council – Information and Strategy Manager
Scope ¹²	See Introduction
Review period ¹³	At least annually
Related Birmingham City Council documents	Data Protection Policy; Information Security Incident Response Standard; Flexible and Remote Access Standard; Disposal of Information Processing Equipment Standard; Asset Management Joint Standard; Information Security Labelling and Handling Standard; Information Security Classification Standard; Personal Data Security Breach Notification Form; Questionnaire for Reporting Loss of Information and other Security Policies, Standards and Codes of Practice.
BS ISO/IEC 27001:2005 BS 7799-2:2005 control references	<i>Control Reference</i> A.7 Asset Management A.8.3.3 Removal of Access Rights A.11.1.1 Access control policy A.11.2.2 Privilege management A 13.1 Reporting Information Security events and weaknesses A 13.2 Management of Information Security incidents and improvements. A.15 Compliance with legal requirements A 15.1.1 Identification of applicable legislation A.15.1.3 Protection of organisational records.

Document History

Version. Amendment	Date	Purpose	Author
5.1	16/02/2012	Annual Review	Jill Walker
5.2	27/02/2012	Amendments following review comments	Jill Walker
6.0	01/03/2012	Approved by BTCG	Caroline Hobbs

Document Distribution after Approval

Version	Name	Organisation
6.0	All Staff	BCC/SB

Document Reviewers

Version	Date	Name	Organisation
5.1	24/02/2012	CISG	BCC/SB

Document Approval by Birmingham City Council

Version	Date	Name	Role
5.0	24/02/2011	BTCG	Authorising body
6.0	01/03/2012	BTCG	Authorising body

¹⁰ AUTHORITY: The person or organisation who is responsible for enforcing this Standard.

¹¹ OWNER: The organisational position of the person who has rights to authorise changes to, or disposal of this Standard.

¹² SCOPE: The organisations or persons to whom the Standard applies.

¹³ REVIEW PERIOD: How frequently the Standard should be reviewed.