Birmingham City Council

Internet Monitoring Standard

If you have any 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 Performance and Information Division, Birmingham City Council
Author:	Richard Green Manager – Security SP&BS Team, Service Birmingham
Version:	6.0
Date:	22/08/2013
Classification:	NOT PROTECTIVELY MARKED

Produced in conjunction with

CONTENTS

1. OVERVIEW AND PUBLICATION PARTICULARS

Document History

Version	Date	Purpose	Author
Draft 1	10/01/2006	Network Security Team discussions	Sue Smith
Draft 2	16/01/2006	Network Security Team amendments	Sue Smith
Draft 3	18/01/2006	Information Security Team amendments	Sue Smith
Draft 4	14/03/2006	CISG amendments	Sue Smith
Draft 5	03/04/2006	Further CISG amendments	Sue Smith
Draft 0.6	18/01/2007	Completely rewritten	Madeleine Westrop
Draft 0.7	09/02/2007	Changes after comments from Audit	Madeleine Westrop
draft 1.0	09/03/2007	Submitted for approval	Madeleine Westrop
1.0	24/04/2007	Approved by BTAG	Caroline Hobbs
2.0	22/04/2009	Approved by BTAG	Caroline Hobbs
2.1	22/06/2010	Annual review	Richard Green
2.2	30/06/2010	Finalised following review comments	Richard Green
3.0	07/07/2010	Approved by BTAG	Caroline Hobbs
3.1	27/06/2011	Annual review	Richard Green
3.2	06/07/2011	Revised following comments from reviewers	Richard Green
4.0	23/08/2011	Approved by BTCG	Caroline Hobbs
4.1	27/07/2012	Annual review	Richard Green
4.2	15/08/2012	Revised following review period	Richard Green
5.0	22/08/2012	Approved by BTCG	Caroline Hobbs
5.1	31/07/2013	Annual review	Richard Green
5.2	13/08/2013	Finalised following end of review period	Richard Green
6.0	22.08/2013	Approved by BTCG	Caroline Hobbs

Standard Distribution after Approval

Name	Organisation
All staff	Birmingham City Council
All staff	Service Birmingham

Standard Reviewers

Name	Organisation	Role
CISG members	BCC/SB	Author/Reviewer

Standard Approval

Name	Organisation	Role	Date
BTCG	Birmingham City Council	Authorising Body	22/08/2013

Overview

Authority[1]	Birmingham City Council – Assistant Director Performance and Information Management Division
Owner[2]	Birmingham City Council – Information and Strategy Manager
Scope[3]	Identical to the scope of the Internet Use Policy
Review period[4]	This document will be reviewed at least annually.
Related documents	Internet Use Policy Internet Use Code of Practice Glossary and Appendix to the Internet Use Policy Blocked Internet Category Procedure Request for access to a blocked Internet category E-mail Use Policy E-mail Use Code of Practice Investigation Access Procedure Human Rights Act 1998 Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000

BS ISO/IEC 27001:2005
BS 7799-2:2005
control references

Control Reference	
A7.1.3	Acceptable use of assets
A8.2.2	Information security awareness, education and training
A10.3.1	Capacity management
A10.4	Protection against malicious and mobile code
A10.8	Information exchange policies and procedures
A10.9	Electronic commerce services
A10.10	Monitoring
A.13.2	Management of information security incidents and improvements
A15.2.1	Compliance with security policies and standards

[1] AUTHORITY: The person or organisation who is responsible for enforcing this standard

[2] OWNER: The organisational position of the person who has rights to authorise changes to, or disposal of, this standard

[3] SCOPE: The organisations or persons to whom the standard applies

[4] REVIEW PERIOD: How frequently the standard should be reviewed

2. INTRODUCTION

2.1 Purpose of the Internet Monitoring Standard

This Standard is published in order to make it clear to all Internet users that Birmingham City Council monitors and reports on use of the Internet in a fair and appropriate way.

The purposes of the Standard are to:

- set out the reasons why Internet use is monitored;
- explain the types of information which are recorded as part of the council's monitoring of Internet use;
- provide information about the types of Internet monitoring reports that are produced and about how monitoring information may be used.

Appendix 1 below provides a one-page summary of this Standard for ease of reference.

2.2 Why Internet use is monitored

Internet use is monitored in order to:

- analyse the use of Internet resources and manage those resources;
- control security risks, and in particular to protect the confidentiality, integrity and availability of council information;
- regulate the use of the Internet and make sure it is used in compliance with the council's policies, standards and codes of practice;
- make sure that excessive personal use of the Internet does not:
  - ◇ use up the resources needed by the council;
  - ◇ adversely affect the conduct of council business;
- establish the existence of other facts relevant to the business;
- regulate the way the Internet is used in compliance with the law;
- perform public duties such as those required in the interests of national security or public safety.

2.3 The basis for monitoring Internet activity

All monitoring is carried out in accordance with the ISO27001 Standard for Information Security Management and in accordance with the law. In particular, the Lawful Business Practice Regulations[5] allow the council to monitor its own communications systems in order to establish whether council policies, codes of practice and rules are being followed and whether standards are being achieved.

[5] The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000

2.4 Internet monitoring and other council policy

This Standard is part of the council's set of corporate security standards, policies and codes of practice. Users of the council's Internet service should be aware of, and follow, the related documents which are listed in the *Glossary and Appendix to the Internet Use Policy*. The *Glossary* and all the related documents listed in it can be found on the PSPG database on Lotus Notes or via Inline.

3. INFORMATION RECORDED AS PART OF MONITORING

All traffic to and from the Internet is automatically logged by the council's Blue Coat proxy management software.

3.1 Access to the Internet

The following details are recorded and retained in a log, whenever the Internet is accessed through a Birmingham City Council connection:

- the identity[6] used to access the Internet;
- the date and time the Internet is accessed by that identity;
- the duration of access by that identity;
- the web sites and addresses visited through the Internet by that identity;
- attempts by that identity to access web sites which are blocked[7];
- details about which computer is used to access the Internet by that identity.

3.2 Files downloaded from the Internet

When files are downloaded from the Internet[8], the following details are recorded and retained in a log:

- the names and file types of files downloaded;
- the sizes of files downloaded;
- the web sites and addresses from which files are downloaded;
- the dates and times that files are downloaded from the Internet.

These details are recorded in addition to the standard information listed in section 3.1 above.

3.3 Private use

Private use of the Internet is not treated any differently from business-related use in terms of types of information recorded in logs. All Internet activity, whether business-related or private, is recorded in the same way. Routine reports on Internet use provided to management do not specifically exclude information about private use.

Detailed information about private use may be made available to specific managers and to Birmingham Audit as part of an investigation conducted under the Investigation Access Procedure. However, there are controls applied to such investigations: private information is examined as part of an investigation only where the degree of intrusion is clearly justified and not excessive, in order to investigate or prevent criminal activity, breach of policy, wrongdoing or public harm.

[6] This could be the identity of a person or the identity of a machine (e.g. an IP address).
[7] For information about blocking of access to sites, refer to the *Blocked Internet Category Procedure* on the PSPG database.
[8] The *Internet Use Policy* and *Internet Use Code of Practice* contain restrictions on the types of files which are allowed to be downloaded from the Internet. Any attempts to circumvent these restrictions will be recorded in the logs of Internet activity.

3.4 Internet-based e-mail accounts

If you use a web-based e-mail account through a Birmingham City Council Internet connection, this fact will be recorded and retained in a log. In addition, information relating to e-mails sent and received may be stored within temporary Internet files on your computer. This information may be disclosed as part of an investigation, but only where this degree of intrusion is justified. (Monitoring of internal e-mail sent via Lotus Notes or Microsoft Outlook is not covered by this Standard.[9])

3.5 Temporary Internet files

When you access the Internet, information is stored in temporary Internet files on your computer. This may include private information, such as log-on details for specific websites. This information is not available in the log files, but it could be disclosed as part of an investigation conducted under the Investigation Access Procedure (see section 4.2 below).

3.6 Retention periods for logs

Raw data from the Internet logs will be kept for a period of two years, during which time it will be available for reports or investigations as required.

When Internet log information is made available as part of an investigation conducted under the Investigation Access Procedure, that information will be retained for a period of six years from the date it was prepared for investigation.

[9] Refer to the *E-mail Use Policy* and *E-mail Use Code of Practice* on the PSPG database for information about monitoring of internal e-mail.

4. REPORTS ON INTERNET ACTIVITY

4.1 Management reports

The following standard reports are produced each month, based on information recorded in the Blue Coat logs, and provided to nominated managers for action:

- top 20 and top 50 users, both overall and split between core and non-core time;
- top 20 and top 50 sites visited, both overall and split between core and non-core time;
- top 20 and top 50 users for each Blue Coat category, both overall and split between core and non-core time;
- month on month comparison of the top 50 users;
- month on month comparison of the top 50 sites visited.

"Core time" means Internet Reporting Core Hours (10:00 to 12:00 and 14:00 to 16:00).

In addition, ad-hoc reports may be requested by Internal Audit or council managers for specified teams including any of the information that is logged by Blue Coat. Information about specific individuals must be requested using the Investigation Access Procedure (see section 4.2 below).

Internet reports will be kept in line with the council's Corporate Retention Schedules available on Inline.

4.2 Investigation Access

If analysis of management reports raises a reasonable suspicion of wrongdoing by a particular individual, more detailed and specific information relating to the individual's use of the Internet may be produced under the Investigation Access Procedure. This may include not only information contained in the Blue Coat logs, but forensic information obtained via an analysis of the individual's computer.

More information about the Investigation Access Procedure is available on the PSPG database on Lotus Notes and via Inline.

5. APPENDIX 1: ONE-PAGE SUMMARY

This summary of the Internet Monitoring Standard is provided for ease of reference. It starts with an explanation of the overall purpose of the document, followed by a series of summary paragraphs which are cross-referenced to the numbered sections of the document.

Overall purpose	
This Standard is about how and why Birmingham City Council records and monitors Internet use. It explains why the council records information about this use, what sort of details are recorded and what sort of reports are produced based on this information.	
	details in this section
Who and what is affected by this Standard	
This Standard applies to all Internet access that takes place through Birmingham City Council Internet connections, excluding access that is provided for the general benefit of the public (for example, in libraries). It applies to everyone who uses this access: this includes everyone who works for or with Birmingham City Council, whether employed by the council or not. It covers both business-related and private use of the Internet.	**1**
Why recording and monitoring takes place	
The council provides access to the Internet primarily to assist those who work for it (or with it) to carry out the business of the organisation. Use of the Internet is recorded and monitored for reasons connected to this objective. Recording and monitoring takes place to manage Internet resources so that they are available for the intended purpose and to control risks that might have an effect on the information the council needs to carry out its business. In addition, the council needs to know whether people who are using the Internet are doing so in a way that complies with the organisation's rules. The council may also need to know about Internet use as part of performing its public duties.	**2**
The type of information recorded	
Whenever the Internet is accessed through a Birmingham City Council connection, information is automatically recorded about: who (which person) or what (which computer) is making that connection; when it takes place; how long it lasts; the web sites and addresses visited; and the names, file types and sizes of any files downloaded. This information is recorded regardless of whether the Internet access is business-related or whether it is private use. The information is retained for two years as standard. Information that is extracted from the logs as part of a formal investigation is retained for a longer period.	**3**
Reports that are produced	
Every month, standard reports about Internet use are produced and circulated to managers. These reports show which websites are visited most frequently, which users are making most use of the Internet (both in general and for different categories of website), and comparisons between the current month's statistics and the previous month's. The reports distinguish between use that takes place in core time and in non-core time. If there is a reasonable suspicion of wrongdoing by a user of the council's Internet service, then a formal investigation may be started and more detailed and specific information about that person's Internet activity may be produced.	**4**