



Birmingham City Council

Internet Use Policy

This Policy is supplemented by an *Internet Use Code of Practice* and a *Glossary and Appendix to the Internet Use Policy* which should be read in conjunction with this Policy. There is also an associated *Internet Access Request Form*.

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

Policy Owner: Gerry McMullan
Information & Strategy Manager, Performance and
Information Division, Birmingham City Council

Author: Jill Walker
Manager – Security
SP&BS Team, Service Birmingham

Version: 6.0

Date: 21/06/2012

Classification: NOT PROTECTIVELY MARKED

© Birmingham City Council 2012



Produced in conjunction with

CONTENTS

1. OVERVIEW AND PUBLICATION PARTICULARS	3
Overview	4
2. INTRODUCTION.....	5
2.1 Scope of the Internet Use Policy.....	5
2.2 Ownership and administration of this Policy	5
3. OBJECTIVES OF THE INTERNET USE POLICY	6
3.1 Security	6
3.2 Monitoring, discipline and complaints	6
3.3 Good reputation and council Policy	6
4. INTERNET USE POLICY RULES.....	7
4.1 Authorised Internet Users	7
4.2 Prohibited activities and sites.....	7
4.3 File transfers	8
4.4 Private use	8
4.5 Personal access control must always be maintained.....	8
4.6 Network security must be maintained	8
4.7 Only Service Birmingham can connect the council’s network to the outside world.....	9
5. INTERNET USE ADMINISTRATION RULES.....	10
5.1 Monitoring and reporting	10
5.2 Internet blocking.....	10
5.3 Complaints	10
5.4 Discipline.....	10

1. OVERVIEW AND PUBLICATION PARTICULARS

Document History

Version	Date	Purpose	Author
1.0	November 2006	Final Version after reviewer comments and approval meeting	M Westrop
2.0	March 2007	Final Version after Councillor Alan Rudge Comments	D Thomas
3.0	April 2009	Approved by BTAG	J Walker
4.0	June 2010	Approved by BTAG	C Hobbs
4.1	13 May 2011	Annual Review	J Walker
4.2	27 May 2011	Amendments following review comments	J Walker
5.0	20 July 2011	Approved by BTCG	C Hobbs
5.1	23 May 2012	Annual Review	J Walker
6.0	21 June 2012	Approved by BTCG	C Hobbs

Policy Distribution after Approval

Name	Organisation
All staff	Birmingham City Council
All staff	Service Birmingham

Policy Reviewers

Name	Organisation	Role
CISG members	BCC/SB	Author/Reviewer

Policy Approval

Name	Organisation	Role	Date
BTCG	Birmingham City Council	Authorising Body	21 June 2012

Overview

Authority	Birmingham City Council – Assistant Director Performance and Information Division
Owner	Birmingham City Council – Information & Strategy Manager
Scope	See Introduction below
Review period	Annual
Related documents	Internet Use Code of Practice Glossary and Appendix to the Internet Use Policy Internet Access Request Form Password Control Standard Internet Monitoring Standard

BS ISO/IEC 27001:2005	<i>Control Reference</i>
BS 7799-2:2005	A5.1 Information Security Policy
control references	A7.1 Responsibility for assets
	A7.1.3 Acceptable use of assets
	A8.2 Human resources security during employment
	A10.3.1 Capacity management
	A10.4 Protection against malicious and mobile code
	A10.8 Exchange of information
	A10.9 Electronic commerce services
	A10.10 Monitoring
	A15.2 Compliance with security policies and standards, and technical compliance

2. INTRODUCTION

2.1 Scope of the Internet Use Policy

This Internet Use Policy applies whenever Birmingham City Council provides an Internet service, with the exception of Public Access Internet provision¹. It applies whenever the Internet is accessed through a Birmingham City Council connection, whether the computer equipment is owned by Birmingham City Council or not.

This Policy applies to all those who benefit from Birmingham City Council's Internet Service: to employees; to temporary and agency staff; to contractors; to all third parties working for the council; to partners in joint ventures with the council; to Elected Members; to volunteers and any other parties using the council's Internet service. This Policy applies to these parties whatever their purpose, whether or not the Internet connection is for their work or for private use. All use of the Internet must be in accordance with this Policy and related policies.

This Policy is an integral part of the council's corporate security policies which are published on the PSPG database and which are also available via Inline.

In line with the Government Connect Code of Connection all users must access the Internet via the Blue Coat Proxy Server and be formally authenticated by accepting the Internet Use Policy.

2.2 Ownership and administration of this Policy

Birmingham City Council owns and administers the Policy.

Service Birmingham is responsible for managing Internet technology for Birmingham City Council; Service Birmingham manages the technology in compliance with this Policy.

¹ See the *Birmingham City Council Policy on Public Internet Access* available on the PSPG database.

3. OBJECTIVES OF THE INTERNET USE POLICY

3.1 Security

This Policy is intended to minimise security risks. These risks might affect the council's information resources and IT equipment, the [Authorised Internet User](#) and the public. In particular these risks arise from:

- hacking and other unauthorised access to council systems or other computer systems;
- the wrongful disclosure of private, sensitive², privileged, confidential and commercially sensitive information;
- the exposure of council systems to malicious or harmful software;
- the use of council systems to access inappropriate or offensive material (and other risks such as bullying or fraud associated with such inappropriate material);
- exposure of the council to vicarious liability for commitments made by individuals on the Internet.

3.2 Monitoring, discipline and complaints

This Policy aims:

- to make it clear to all Internet users that fair and appropriate levels of monitoring and reporting are carried out (see [Monitoring and reporting](#), below);
- to make it clear that disciplinary procedures (see [Discipline](#), below) will be used against individuals who contravene this Policy;
- to clarify the procedure for complaining about all aspects of Internet use (see [Complaints](#), below).

3.3 Good reputation and council Policy

To support various council policies and duties, access to certain web sites is restricted: particularly those which display criminal, hate, sexually explicit, racist and other inappropriate material (see [Prohibited activities and sites](#), below).

This Policy aims:

- to protect the good reputation of Birmingham City Council;
- to promote best use of Internet facilities for achieving the council's objectives.

² Sensitive information: see *Glossary and Appendix to the Internet Use Policy*.

4. INTERNET USE POLICY RULES

4.1 Authorised Internet Users

The council's Internet facilities are provided for council business purposes and access must be authorised by an appropriate manager, as set out in the *Internet Use Code of Practice*. Access is granted only on condition that the individual formally agrees to the terms of this Policy and the related Code of Practice. The authorising manager must confirm that there is a legitimate business need for access which must be stated on the *Internet Access Request Form*. A copy of the form must be held locally by the individual and the manager and kept for audit purposes.

Requests for access to the Internet must be made to Service Birmingham using the SLAM process.

4.2 Prohibited activities and sites

Access to some Internet sites and categories of site is blocked (see [Blocking](#), below).

Certain activities and Internet sites are prohibited to safeguard the Internet service and to further the objectives of this Policy (see [Objectives](#)). More detail about prohibited activity is contained in the Internet Use Code of Practice. The following prohibitions are particularly important for these Policy reasons.

Internet users **must not**:

- use Internet facilities to break the law or incite crime;
- gain unauthorised access, or make unauthorised modifications, to computer material (hacking);
- use another individual's user identity or password;
- enter into contractual obligations on behalf of the council over the Internet, unless the transactions are formally authorised in writing by line managers having acted in accordance with the approved corporate procedure;
- display, access, use, extract, store, distribute, print, reveal or otherwise process information which contravenes the law or council policies, particularly policies on harassment and discrimination;
- distribute copyright material in breach of copyright;
- distribute defamatory material³;
- unlawfully disclose any sensitive business information, commercially sensitive information or personal information;
- transfer information with a classification higher than NOT PROTECTIVELY MARKED over the Internet;
- attempt to access sites which are blocked (see [Blocking](#), below);
- try to circumvent any of the controls which block access to Internet sites.

Any employee who uses IT resources for illegal activity will be disciplined and the activity will be reported to law enforcement agencies. Any employee who uses IT resources for the distribution of defamatory material will be disciplined.

³ Refer to the *Internet Use Code of Practice* for more information.

4.3 File transfers

Birmingham City Council allows [Authorised Internet Users](#) to transfer **information** files from the Internet to computer equipment under certain conditions. Refer to the *Internet Use Code of Practice* for detail about information file transfers.

Software **must not** be downloaded from, or uploaded to, the Internet.

4.4 Private use

Some private use, which is not related to council work, is allowed within certain limits as described in the *Internet Use Code of Practice*. This is to be viewed as a privilege and, if there is evidence of abuse, appropriate disciplinary action will be taken against individuals concerned. Abuse is any deliberate infringement of this Policy, or the associated *Internet Use Code of Practice*.

All Internet use, whether business-related use or private use, will be monitored and reported on as described [below](#).

4.5 Personal access control must always be maintained

Internet users must follow the password guidelines in the Password Control Standard.

4.6 Network security must be maintained

No attempt must be made to disable, defeat or circumvent council firewalls⁴ or similar network security facilities. Note that the council's firewall software can automatically disconnect Internet connections when this is necessary to protect the service.

No Internet user may use the Internet deliberately to propagate any virus, worm, Trojan Horse, spyware, malicious code or unauthorised mobile code.

⁴ Firewalls: see *Glossary and Appendix to the Internet Use Policy*.

4.7 Only Service Birmingham can connect the council's network to the outside world

Service Birmingham must authorise all technological applications and peripherals, including telephones and cameras, which connect to the Internet through Birmingham City Council Internet connections. Written authorisation may be obtained through the Service Birmingham Service Desk⁵.

Service Birmingham must always manage any connection which links the council's network to the outside world. Internet Users are **not** allowed independently to connect PCs or servers, which are already connected to the Birmingham City Council network, to the Internet or to any other external system.

In exceptional circumstances, connections may be allowed which are not supplied through Service Birmingham, but through independent dial-up devices (modems) or other methods. These exceptions must always be authorised through the Service Birmingham Service Desk and will not be accepted unless they comply with the Government Connect Code of Connection.

Internet connections using the council's telephone network are **not** allowed.

⁵ Service Birmingham Service Desk – telephone 4/4444

5. INTERNET USE ADMINISTRATION RULES

5.1 Monitoring and reporting

All use, whether business-related or private, will be monitored continuously by Service Birmingham in line with the *Internet Monitoring Standard*. Reports on activity will be produced on a monthly basis detailing usage trends, individual top users and top categories of sites visited. These reports will be circulated to nominated business managers who may request more in-depth reports or perform individual investigations as necessary.

All use of the Internet both business and private will be recorded and reported on, as detailed in the *Internet Monitoring Standard*. Internet Users must acknowledge their consent to the *Internet Monitoring Standard* when they apply for Internet Access (see the *Internet Access Request Form*).

5.2 Internet blocking

In order to implement this Policy and to further its [objectives](#), the council reserves the right to block access to certain Internet sites/categories without warning. Service Birmingham may also take temporary measures to block or change the access to a particular Internet site/category. All blanket decisions about access are council business decisions and must ultimately be confirmed by the Business Transformation Co-ordination Group (BTCG).

5.3 Complaints

Anyone who wishes to complain about the Internet service provided by the council, or raise the question of whether a particular Internet site should be blocked, should follow the complaints procedure set down in the *Internet Use Code of Practice*.

5.4 Discipline

Any Internet User who contravenes the rules in this Policy or the associated *Internet Use Code of Practice* will be disciplined under the council's disciplinary procedure wherever this is appropriate for that user (see the *Internet Use Code of Practice*). It is possible that the disciplinary procedure can result in dismissal. When there is evidence of a criminal offence, the police will be informed.