Doncaster
Metropolitan Borough Council

Internet Usage Policy

29th February 2012
V2.5
N. Minnikin

Document Control

Document Location

The source of the document will be found at :

S:\ICT\Information Management\Policies\New Policies\Internet Usage\InternetUsage policy V2.5

Revision History

Date of this revision 29th February 2012
Date of next revision February 2013

Revision Date	Revision Version	Prev Revision Date	Prev Version	Summary of Changes
January 2003	1.6	N/A	N/A	Revised to cater for employees using Internet for personal use (ITSG 30 January 2003)
March 2007	2.0	January 2003	1.6	Reviewed / rewritten in line with new security standard, changes in use of Internet and new Acceptable Use Policy
May 2007	2.1	March 2007	2.0	Amended for Comments from Employee Relations Committee Brief.
June 2007	2.2	May 2007	2.1	Amended for Comments from Audit Committee Brief
October 2007	2.3	June 2007	2.2	Amended to correct wording regarding productive business hours.
March 2009	2.4	October 2007	2.3	Amended to amend statements regarding the acceptable and prohibited use of Internet
February 2012	2.5	March 2009	2.4	Amendment to • Page 4 – Acceptable Use of the Internet – Addition of the final paragraph. • Page 5 – Prohibited Use of the Internet – First Bullet Point – Remove ‘excessive’. • Page 6 – Social Networking – Amended to reflect the ability to use Social Networking sites for work purposes and whilst clocked out.

Distribution

This document has been distributed to

Name	Title	Date of Issue	Version
Intranet		February 2012	2.5

Introduction and Scope

The Council provides members and staff access to the Internet in order to help communications with external bodies and to enable effective research and development to be carried out.

The Council has a duty to inform all Internet users:

- of the rules to be applied when using the Internet
- of their responsibilities
- what is defined as acceptable use
- what would constitute misuse
- of the consequences of abuse

This policy applies to ALL staff and members of the Council accessing the Internet using the Council's equipment/software.

This policy also applies to any independent contractors, consultants and other third parties who have been given access to the Internet when using Council's equipment and software.

This policy does not cover the use of e-mail, see the **E-mail Usage Policy** for more details.

Glossary of Terms

For the purposes of this policy:

- 'use' is defined as establishing electronic data communications with the Internet
- 'material' refers to all forms of communications including narrative descriptions, graphics (including photographs, illustrations, images, drawings, logos), executable programs, video recordings, and audio recordings.
- 'abuse' is defined as any action that constitutes illegal or unacceptable behaviour and is strictly prohibited.

Responsibilities

All members, staff and other third parties who have been provided with access to the Internet should be aware of their responsibilities when using this facility. These responsibilities include:

- adhering to this policy
- reporting any network or Internet misuse to an appropriate Senior Manager, Director of Information & Communication and, where necessary, Audit Services
- not violating the Council's **E-mail Usage** and **Acceptable Use** policies

The use of a 'password screen saver' shall not be considered sufficient protection. It is essential that you always 'lock' your screen by pressing 'Ctrl Alt Delete' and then enter to confirm that you wish to 'lock' your workstation.

Acceptable Use of the Internet

The following are examples of what is considered to be acceptable use of the Internet:

- communication with government or local government personnel, vendors, and other private businesses
- communications, including information exchange, for professional development or to maintain relevant knowledge or skills
- activities involving government advisory or standards activities
- communications for administrative purposes
- use for authorised training purposes
- approved research and development purposes
- where employees are required to provide support and assistance to the general public as part of their duties, then they must still adhere to this policy, but are allowed to access non-work related sites on behalf of members of the public.

All of the above must be relevant to the user concerned and required for the user to perform their duties efficiently.

Personal use of the Internet is limited to lunch breaks and work breaks only. All employees must ensure that they are logged out (clocked out) of flexitime when using the internet for personal use. Employees may not use the Internet for personal use during otherwise productive business hours. If employees do use the internet for personal use whilst being clocked in, this may be classed as misconduct / gross misconduct, dependent upon the excess and seriousness.

Whilst personal use of the internet is permitted during lunch and work breaks, staff and members must be aware that internet facilities are provided by the

Council – anything that staff and members would not want to be monitored, should not be conducted on the Council provided internet facility.

It must be noted that the internet is not a secure medium. Users sending their own personal, financial, sensitive or confidential material do so at their own risk and the council accepts no responsibility for any loss.

The council is not liable for any losses or disputes resulting from on-line banking, shopping or trading in stock & shares etc. Users participate in these activities at their own risk and must indemnify the Council against any claim or demand against them as a result of their activities.

User should not make comments about the Council or display themselves as a Council employee on the internet unless they state that their views are their own and not the views of the Council.

Prohibited Use of the Internet

Abuse of Internet access is classed as a disciplinary offence, for which staff may be subject to disciplinary action. Users are reminded that any suspicion of abuse will be monitored

The following are examples, within broad limits, of the type of abuse of Internet access which may constitute Gross Misconduct in accordance with the Council's disciplinary rules and would lead to disciplinary action being taken:

- personal use of the Internet whilst being clocked in for work
- use for private business and / or gain
- use of the Internet to knowingly transmit, receive or search for material which is unlawful, indecent, objectionable, offensive, obscene, abusive, threatening or defamatory
- the storage of material downloaded from the Internet on any storage medium (network drive, PC drive, CD, etc.) which
    - is unlawful, indecent, objectionable, offensive, obscene, abusive, threatening or defamatory (accessed either knowingly or inadvertently)
    - does not directly relate to an individual's specific area of work and responsibility
- publishing personal information, such as the home address, telephone number, or financial data of another person without their consent or without a legal basis to do so
- accessing, transmitting, receiving or searching for confidential information about another person without their consent or without a legal basis to do so
- downloading or transmitting the Council's confidential information without authorisation
- downloading or transmitting copyrighted materials without the permission of the copyright holder. See also **Acceptable Use Policy**
- interfering with or disrupting network users, services, security measures or equipment
- using the network to gain unauthorised entry to another PC or mobile

device on a network
- any activity that is illegal in any jurisdiction
- use of the Internet to promote otherwise legal material with which the Council concludes, in its sole discretion, it does not want to be associated with in order to protect its reputation and standing, or to protect its elected Members and staff.

The list is neither exhaustive nor exclusive.

Social Networking Websites

The use of Social Networking web sites e.g. Facebook/Twitter, for work purposes are permitted. However, staff who do access these sites need to be mindful not make comments or express an opinion unless these are shared by the Council.

Personal use of the Social Networking web sites e.g. Facebook, Twitter is limited to lunch breaks and work breaks only. All employees must ensure that they are logged out (clocked out) of flexitime when using these sites for personal use, either by PC or Smartphone. Employees may not use these sites for personal use during otherwise productive business hours. If employees do use these sites for personal use whilst being clocked in, this may be classed as misconduct / gross misconduct, dependent upon the excess and seriousness.

Users are reminded that any suspicion of abuse will be monitored.

Inadvertent Abuse of the Internet

It is recognised by the Council that staff and members may, during acceptable use of the Internet, make inadvertent access to a site or page which contains material which is unlawful, indecent or objectionable. In these circumstances staff should disconnect from the Internet immediately, and notify their line manager as soon as possible after the incident, providing details of the date and time of the inadvertent access. Reconnection to the Internet should be deferred until this action has been taken. The **e-form** available on the intranet should be used to record details of inadvertent access so that they may be made available for the purpose of internal or district audit should the need arise. In instances where the officer concerned is a Chief Officer and there is no line manager to report the incident to then an entry should be made in the declarations log before reconnecting to the Internet.

Any suspicion of abuse must be reported to an appropriate Senior Manager, Director of Information & Communication and, where necessary, to Audit Services.

Privacy of the Internet

Users are reminded that the Council has the legal right to monitor the usage of the Internet system. This will be undertaken where there is suspicion of abuse or misuse of the Internet system and random checks may be carried out. It will be authorised by the Director of Information & Communication and carried out under the guidelines of the Regulation of Investigatory Powers Act 2000 (RIPA).

Whilst personal use of the internet is permitted during lunch and work breaks, staff and members must be aware that internet facilities are provided by the Council – anything that staff and members would not want to be monitored, should not be conducted on the Council provided internet facility.

Further Guidance

Further guidance can be found via the **link** on the front page of the council's intranet site or by putting a call on the ICT Helpdesk 7(3)4356.