



Leicester
City Council

Information Assurance Policies and Guidance

Acceptable Use Policy for Use of the Internet

1 December 2009

**Document Version: V1
Review Date: 1 December 2010**

Owner: Head of Information Security

Document History

Revision Date	Version Number	Summary of Changes

Aim

1. To ensure all users of Council provided internet facilities are aware of and adhere to the requirement for the acceptable use of such facilities.

Applicability

2. This Policy applies to all Users of Council ICT Systems and Services and is to be applied at all times whenever using the Council provided Internet facility. This includes access via any device including desktop computers and mobile devices. Provision of internet access to Schools is subject to separate controls in line with national standards to be applied in the education sphere.

Review and Maintenance

3. This Policy is agreed and distributed for use across the Council by the Information Management Programme Board (IMPB) on behalf of the Operations Board. It will be reviewed annually by the Head of Information Security, who will forward any recommendations for change to the IMPB for consideration and distribution.

Scope

4. This policy covers how you should use your Council Internet facility. It outlines your personal responsibilities, what is permissible and what is not.
5. The Internet facility is made available for the business purposes of the Council. A certain amount of personal use is permitted in accordance with the statements contained within this Policy. Personal use is defined as use of the internet for any purpose which is not directly related to the individual's role or the Council's business.
6. It is recognised that it is impossible to define precise rules covering all Internet activities available and adherence should be undertaken within the spirit of the policy to ensure productive use of the facility.
7. This policy updates the Council's Security Policy for Internet Web Services - Content Filtering dated 1 February 2008 and replaces all previous locally agreed Internet usage policies and practices.

Risks

8. The Council recognises that there are risks associated with users accessing and handling information in order to conduct official Council business.
9. This policy, in conjunction with other Information and ICT Security policies and controls, aims to mitigate the following risks:
 - the introduction of malware in any form onto the Council ICT estate
 - the loss or exposure of Council data
 - the non-reporting of information security incidents
 - the loss of direct control of user access to information systems and facilities etc.
 - reputation loss and damage through inappropriate use by staff
 - loss of productivity through ineffective time management and usage of facilities paid for from public funds
10. Non-compliance with this policy:
 - would have a significant effect on the delivery of Council services to our customers or internally and may result in data or financial loss;
 - gives rise to the risk of prosecution or other liability to the individual and the Council

Applying the Policy

What is the Purpose of Providing the Internet Service?

11. The Internet service is primarily provided to give users:
 - Access to core ICT services that are internet dependent eg external email exchange
 - Remote access facilities
 - Access to external information and services that are pertinent to fulfilling the Council's objectives and priorities.
 - The capability to post updates to Council owned and/or maintained web sites.
 - An electronic commerce facility.

Internet Account Management, Security and Monitoring

12. The Council provides a secure network logon-id and password account facility to access the Internet. The Council's Information & Support Division (Technology Services) is responsible for the technical management of this account.

13. You are responsible for the security provided by your Internet account logon-id and password. Only you should know and use your log-on id and password as activity is recorded against that detail.
14. The provision of Internet access is owned by the Council and all access is recorded, logged and interrogated for the purposes of:
 - Monitoring total usage to ensure business use is not impacted by lack of capacity.
 - The internet filtering system monitors and records all access for reports that may be produced for management and audit purposes.
16. The Council uses a URL filtering system to block unacceptable types of sites e.g. pornography, gambling, malicious and illegal sites etc. Other sites and categories of sites such as eBay and social networking sites are generally blocked unless access is required to support the needs of a business stream.

What You Should Use Your Council Internet Account For

17. The Council provides internet access to staff as a tool to help staff in their work, your Council Internet account should be used in accordance with this policy.

Personal Use of the Council's Internet Service

18. At the discretion of your Head of Service, and provided it does not interfere with your work, the Council permits personal use of the Internet in your own time, this means after you are clocked out if on flexi time, and for other employees means outside of your normal working hours and in formally designated breaks such as lunch breaks. Any such usage agreement is to be recorded by the Line Manager on behalf of the Head of Service.
19. The Council is not in anyway responsible for any personal transactions any employee enters into or for any claims arising out of personal transactions. Also, only personal and not Council details should be used when making personal internet transactions.
20. Any personal email exchange is to be through a personal web-based, email service and not your Council email account. It should be noted that your Council email account is solely for LCC business and not personal use. Similarly LCC business is not to be conducted using a personal email account.
21. You must ensure that goods and services purchased for personal use are not delivered to Council property.
22. Your computer and any data held on it or any connected device are the property of Leicester City Council and may be accessed at any time by

the Council to ensure compliance with all its statutory, regulatory and internal policy requirements. The Council will monitor internet usage including the websites that are visited, and the frequency and length of time spent on the internet.

23. You must **not** use your Internet access to:
- Create, download, upload, display or access knowingly, sites that contain pornography or other “unsuitable” material that might be deemed illegal, obscene or offensive.
 - Subscribe to, enter or use peer-to-peer networks or install software that allows sharing of music, video or image files.
 - Subscribe to, enter or utilise real time chat facilities such as chat rooms, text messenger or pager programs.
 - Subscribe to, enter or use online gaming or betting sites.
 - Subscribe to or enter “money making” sites or enter or use “money making” programs.
 - Run a private business.
 - Download any software without the agreement of Information & Support Division (Technology Services).
 - Infringe copyright law
 - Post defamatory, salacious or other comments or statements that could undermine the Council’s reputation on internet based information facilities such as Chat Rooms, Blogs, and social networking sites.
24. The above list gives examples of “**unsuitable**” usage but is neither exclusive nor exhaustive. “**Unsuitable**” material would include data, images, audio files or video files that would be illegal to transmit under British law or contravened copyright law, and, material that is against the policies and rules of the Council.

Your Responsibilities

25. It is your responsibility to:
- Familiarise yourself with and abide by this policy before using the Internet facility provided for your work.
 - Assess any risks associated with Internet usage and ensure that the Internet is the most appropriate mechanism to use.
 - Read and abide by all related security policies published in the Staff Handbook area of Insite, in particular:
 - Acceptable Use Policy for the Information Infrastructure
 - Information Security Policy
 - ICT Security Policy.

Line Manager’s Responsibilities

26. It is the responsibility of Line Managers to ensure their staff are aware of this Policy and that the use of the Internet facility:

- Within an employees work time is relevant to and appropriate to the Council's business and within the context of the users responsibilities.
- Within an employees own time is subject to the rules contained within this document.

Whom Should I Ask if I Have Any Questions?

27. In the first instance you should refer questions about this policy to your Line Manager who may refer you to ICT Support Centre (email: it.supportcentre@leicester.gov.uk Tel: NWC (29) 8888) if appropriate. Councillors should refer questions to Members Support in the first instance.
28. You should refer technical queries about the Council's Internet service to the ICT Support Centre (email: it.supportcentre@leicester.gov.uk Tel: NWC (29) 8888).

Policy Compliance

29. If any user is found to have breached this policy, they will be subject to the appropriate Council disciplinary procedure. Misuse of the Council's ICT facilities is potentially gross misconduct under the Disciplinary Procedures and Code of Conduct. If a criminal offence is considered to have been committed further action may be taken with and through the Police to assist in the prosecution of the offender(s).
30. If you do not understand the implications of this policy or how it may apply to you, seek advice from your Line Manager.