LUTON BOROUGH COUNCIL

CORPORATE & CUSTOMER SERVICES DEPARTMENT

INFORMATION & CUSTOMER SERVICES (ICS)

INTERNET SECURITY POLICY

7ι INVESTOR IN PEOPLE 1θ

Internet Security Policy

Introduction

This policy applies to all users of the Luton Borough Council network (excluding members of the general public, or students using the separate Library and Schools networks). Users being full-time and part time employees, home-workers, students, voluntary workers, contractors, 3rd party suppliers and members.

Threats from the Internet pose increasing risks to computer installations and networks regardless of size or location. LBC is not exempt from these threats. Some examples include; virus attacks, which can corrupt data or degrade services, Internet worms which can undermine security, or Denial of Service attacks which flood systems with bogus requests for data, preventing legitimate users from using a service. In response to these threats we have implemented a number of security measures including:

- Educating staff to the pitfalls of the Internet and the consequences of misuse.
- Limiting staff access to the Internet on a 'need to have' basis.
- Regulating access to inappropriate web sites.
- Monitoring of staff Internet use and reporting suspected misuse to Management.
- Scanning web traffic, servers and PCs for viruses, Trojans or other malicious code.
- Limiting use of file transfer facilities e.g. FTP.
- Restricting external access to the LBC network using firewall technology.
- Managing and monitoring systems security in compliance with the British Standard BS7799 Part 2.

Obtaining Internet access

The Council provides the Internet facility exclusively for business use. Occasional personal use is permitted, provided that it does not exceed 60 minutes per week. Personal use is forbidden during your contracted hours of employment, other than during designated breaks. For employees on flexi time, this means no personal use between 10AM and midday and from 2PM till 4PM i.e. core time. In addition, Internet use must not interfere with the performance of your duties. Any abuse will be subject to the normal disciplinary procedures.

Staff undertaking academic development may access the internet (for study purposes) during core hours. This must be with the prior knowledge and authorisation of their Line Manager. Specific times for access should be agreed in this case.

1. Access to the Internet needs to be approved by your Line Manager.

2. If approved, your Line Manager will submit a request for internet access (including the business case behind your requirement) to Information & Customer Service (ICS), who will set-up your internet account.

3. ICS will ask you to read the internet security policy, then sign and return an ' Internet security access form' undertaking to agree by the standards and conditions laid out in this policy.

4. Once the signed 'Internet access form' is received back into ICS, your internet access will be enabled.

Web Awareness

It is important to note that when you visit an internet site you leave traces of your visit in a number of places. These include:

- The web sites you visit
- The web monitoring software used by LBC to manage internet access
- Your history file on your internet browser
- Your 'cookies' file in your PC

  Cookies are placed on your PC when you visit some web sites as you visit them. The cookies allow the sites to build a profile of you as a customer and can be used to send you special offers etc. specific to your customer profile.

We strongly advise against use of web banking (or similar applications) from PCs supplied for use by council employees or members. These applications store personal information e.g. bank account details on the C: drive of your PC. Other users could retrieve this information from your PC and misuse it. LBC will not be held liable for any financial losses that occur as a result of using web banking facilities on the LBC network.

Internet users like all PC users have a responsibility to ensure that the LBC network is kept secure. See The PC security Manual in public folders for further information. In particular, Internet users should be aware of the threat from failing to keep passwords secure. All Internet users have a single user name and password. THESE SHOULD NEVER BE SHARED, not even if requested by a member of ICS or Helpdesk. Where a password is not kept secure, someone could misuse the Internet under your name!

Misuse of the internet

Remember Internet access is provided primarily as a business tool and should not be misused.

Examples of misuse include: -

- Any use prohibited by corporate policy.
- Use for personal business or activity intended to achieve personal financial gain.
- Making confidential information available to unauthorised individuals outside LBC.
- Sending, forwarding, browsing, exporting from or importing any materials that are or could be in any matter whatsoever, considered to be pornographic, obscene, offensive (whether from a sexual, racial, political, religious or any other perspective), defamatory or of a criminal or subversive nature.
- Inappropriate services (as specified in web-site restrictions).
- Downloading and installation of application or executable software without prior approval from Information & Customer Services. Approval can be obtained by contacting the service desk.
- Any use that could bring LBC or its employees into disrepute

This list is not exhaustive.

Any misuse will be pursued by the Council's disciplinary policy.

Web site restrictions

Internet access at LBC is focused on providing access to sites relevant to Council business. In line with this, web access is not provided to sites that can be categorised as follows:

Adult or explicit	Chat	Criminal skills
Drug alcohol or tobacco	Gambling	Games
Glamour/intimate apparel	Hacking	Hate speech
Personals & dating	Usenet	Violence
Web-based mail e.g. hotmail	Weapons	

You may contact the ICS System Administrator for clarification of any of these categories.

If you accidentally gain access a site that falls into one of the categories above, don't panic!
Contact the Service Desk immediately, by e-mail or phone on 6666 and provide them with the site details.
This action has 2 benefits:

(i) It allows us to block this site, preventing other users from accessing it inadvertently
(ii) It highlights to ICS that the you did not intend to access the site.

It should be noted however, that if you fail to contact the Service Desk, or repeatedly visit the in appropriate site, this will be classified as misuse.

Some users will have valid requirements to visit a web site, or category of sites, where access is not normally available. In such cases, details of the requirement should be passed to your line Manager, who can arrange access via the Service Desk.

Internet Monitoring & Reporting

A series of Internet monitoring reports are produced and passed to LBC Management on a regular basis. These reports include analysis of Corporate, Departmental and individual use.

Conclusion

The provision of a corporate connection to the Internet represents a significant threat to the security of the Borough's networked services. Technical measures have been taken to reduce the threat to a bare minimum, but equally important is the cooperation of our staff. By adhering to this policy, you are protecting the LBC network, its contents and the reputation of the council.

If you have any query about day-to-day use of the Internet, email the ICS Service Desk on 6666 for advice.

This document outlines the terms on which Internet access will be provided. By requesting this facility and receiving subsequent access, you are deemed to be accepting these guidelines and any actions that may be taken as a result of inappropriate use.

Information & Customer Services (ICS) have set these procedures to meet the standards set out in the Data Security Guidelines in BS7799. This policy forms part of the Council's requirements for BS7799 certification.