



Live Council Websites

The following Councils are the most recent to have their websites developed as part of the Linking Councils and Communities (LCC) Program:

Shire of Three Springs – www.threesprings.wa.gov.au

Shire of Kent – www.kent.wa.gov.au

Shire of Corrigin – www.corrigin.wa.gov.au

Shire of Katanning – www.katanning.wa.gov.au

Website Development Process

Councils participating in the Linking Councils and Communities (LCC) Program are now in various stages of the website development process. Fourteen Councils have had their websites developed through the Program and another 45 Councils are in the process of developing their new websites.

There are a number of stages involved in the development of Council websites through the LCC Program. To assist Councils to better understand the stages that their website goes through as part of the development process, the LCC team has developed a two page summary document which broadly outlines the steps involved.

A copy of the summary document can be accessed on the Internet & Extranet page of the LCC website at www.linkingcouncils.com.

Manages Services

Through the course of piloting the 'managed services' gateway, several themes have emerged from Councils that are likely to be relevant to other Councils and indeed most contemporary organisations.

These issues have been incorporated into the solution being delivered by the project and include:

Web Browsing Privileges - Do you really want ALL of your staff to have access to absolutely ALL webpages on the internet? Probably not. In which case, you need a tool to help manage the appropriate use of internet access. Council administrators can select the web browsing privileges of their users at an individual level, choosing between "None", "Whitelist Only", "Blacklist Restricted" and "Unrestricted".

If in doubt, use the default, which is "Blacklist Restricted", as this provides access to all of the internet, except for sites which have been deliberately blocked as they are known to contain malicious technical content.

Spyware - Since the early 1990's, most computer users have been well aware of the need for virus scanning software, and the "Nimda" and "Code Red" internet worms raised awareness of the need for network firewalls. In the seemingly never-ending game of counter-measure and counter-counter-measure, a new threat has risen over the last three years, and is now at epidemic levels; the threat is so-called "Spyware" or "Adware".

This sort of software may be downloaded and installed by error, often through those annoying web "pop-ups". Other packages lure end users into installing the software, promising trinkets such as "never have to remember a password again", or "a new joke every day" or "new screen background every day".

Unfortunately, this is malicious software that acts to monitor your use of the computer, including emails received, websites visited, and, in extreme cases ("trojans"), passwords, credit card details and bank account details, and then forwards these details which can be used for malicious purposes. We have observed infections in two thirds of the pilot Councils.

Access to the offending sites can be blocked through correct use of the web browsing privileges functionality provided through the Managed Network Gateway.

Councils should contact their IT support staff for assistance in detecting and removing this spyware. Caution will need to be taken in removing the unwanted software as the latest variants (such as "commonname") alter the PC's default settings to the extent that the PC is unlikely to operate correctly after removal.

Public Access PCs - Some Councils provide one or more PCs for the general public to access; including public access library PCs.

Ideally, these PCs should not be on the same network as the main corporate server(s) and PCs as it is easy to gain access to network passwords and other unsecured data moving across the LAN.

Whilst most users do not have malicious intentions, the problem is that some of the software they install (whether intentionally or otherwise) can easily compromise the security of your network, and the privacy of your ratepayers.

We therefore recommend that:

1. Public Access PCs are kept on a completely separate LAN (a "perimeter network" or "DMZ")
2. Public Access PCs are issued with user accounts that are set for "Whitelist Only" or "Blacklist Restricted" browsing privileges (definitely not "unrestricted"!)
3. Consideration is given to the use of "rollback" software, so that the PC returns to a known state every day, regardless of what occurred the day before.

Further information in relation to these issues is included in the telecommunications frequently asked questions publication available on the telecommunications page of the LCC website at www.linkingcouncils.com.



WESTERN AUSTRALIAN
LOCAL GOVERNMENT ASSOCIATION

LINKING COUNCILS AND COMMUNITIES PROGRAM

Western Australian Local Government Association, Local Government House, 15 Altona Street West Perth WA 6005, PO Box 1544 West Perth WA 6872

Telephone: (08) 9213 2016 Facsimile: (08) 9322 2611 Email: info@linkingcouncils.com Website: www.linkingcouncils.com