

Internet Usage Procedure



Signed: _____

A handwritten signature in blue ink is written over the dashed line. The signature is stylized and appears to be 'P. H. A.'. Below the signature, there is a long horizontal blue line.

Chief Executive.

Number:	DBC_00025	Title:	Internet Usage Procedure
Owner:	Info. Security Officer	Last Review	22 nd Jun 2009

INTERNET USAGE PROCEDURE

Introduction:

Staff and Members using DBC's computer systems to access the Internet do so under an implicit agreement to abide by the rules of this procedure.

Monitoring:

All staff should note that DBC has the capability of monitoring Internet usage on the Council system.

All actual Internet access, or attempted access is recorded. Reports are generated automatically each month, graphing the top 10 Internet user names, the top 25 sites accessed and the top 25 blocked sites attempted. These reports are made available to CMT, ICT management and the Information, Security & Standards Officer.

Reports showing an individual's Internet access will only be generated on request from a senior manager.

DBC recognises the legal consideration of employees' right to privacy, but the council also has an obligation to ensure the system is not being abused in any manner.

Monitoring of the actions of employees without their consent is permitted under the Lawful Business Practice Regulations for certain specified purposes, including: investigating unauthorised use; prevention/detection of crime; to ascertain compliance with regulatory practises relevant to the Council.

Note: if you object to the Council monitoring your personal use of email or internet, then you should refrain from using Council equipment for personal use.

Installation:

Installation and connection to the Internet is only to be performed by DBC's ICT department. Connection will be through the Council's secure firewall, which acts to secure DBC's system from external attack.

No DBC equipment is to be connected to the Internet by the use of a MODEM, unless authorised (and installed) by the ICT department.

Number:	DBC_00025	Title:	Internet Usage Procedure		
Owner:	Info. Security Officer		Last Review	22 nd Jun 2009	

Access to Internet:

Internet access from the DBC network is controlled using firewall and specialist filtering software. This software allows the blocking or un-blocking of sites, either individually, or by type of site, and also handles the internet monitoring and reporting, as specified above. Timed access can be handled to ensure sites can only be accessed during specified times.

Internet sites blocked by the firewall include, but are not limited to, the categories of pornography, paedophilia, racist and hate, music, gambling and gaming. Internet users should be aware that an attempt to access a blocked site is permanently recorded, even if the attempt is successfully blocked.

General Internet access will be given if the individual's manager has requested permission. An individual wanting access to a currently blocked web site should also make the request via their immediate manager.

Individuals should take care about accessing unknown sites:

NOTE: Most Internet sites remember who has accessed their site - every site you access, you may leave a 'calling card' with DBC's name on it, an action which could bring DBC into disrepute.

While the Council accepts that some private use of the Internet is acceptable, this must be kept to a minimum. Private use should be outside of normal working hours, or during lunch breaks. Regardless of hours, certain activities are expressly prohibited, these are:

- Accessing of sites of a pornographic, paedophilic or similar nature. Accessing such sites shall be regarded as gross misconduct, leading to disciplinary action.
(Inform the ICT Helpdesk (x2234) immediately if any such sites are accessed accidentally, the site can then be blocked to prevent further access.)
- Online games playing - these take up an excessive part of the available bandwidth of the Internet link.
- Discussion groups should be accessed only for business reasons.
- Under no circumstances should anything sensitive or confidential be posted on the Internet.
- Under no circumstances should anything in any way defamatory be posted on the Internet. The laws of libel apply to individuals posting such information.

Additionally, downloading (copying) information is liable to the following restrictions:

- Software, other than documents and information, should never be downloaded to a corporate PC/laptop. Specifically, such items as Shareware, freeware and Toolbars are prohibited for the following reasons:

Freeware: Even if free, may come with Corporate use restrictions, and is covered by Copyright law.

Shareware: Subject to Copyright laws after trial period (usually around 30 days)

Number:	DBC_00025	Title:	Internet Usage Procedure
Owner:	Info. Security Officer	Last Review	22 nd Jun 2009

Toolbars (e.g. Yahoo toolbar): Many of these act as spyware, monitoring your internet access, collecting and returning information about you and tailoring pop-up advertisements to your internet activities.

- When downloading documents and information files, remember to adhere to the rules of copyright which applies to them.

Images

No user shall view or download inappropriate images (e.g. images which show violence or are pornographic, obscene, discriminatory or otherwise offensive in nature), or store such images, on any DBC laptop, PC or network drive. Viewing, downloading or storing such images will be regarded as system abuse. Individuals will be subject to DBC's conduct procedure for any such actions and may face dismissal.

User Responsibility:

- Adherence to the above rules regarding Internet access.
- DBC ICT department will make every attempt to recognise, and prevent access to unacceptable sites, but accepts that some sites will be missed. It is also recognised that it is possible to accidentally enter an unacceptable site as a result of an innocent search. In such a case, you should inform the ICT Help Desk on x2234, or by email, as soon as possible, in order for it to be blocked. In such a case, take a note of the full address of the site to send to ICT.
- If you think a virus may have infected your PC or laptop, contact the ICT Help Desk IMMEDIATELY on x2234. Do not use the PC until ICT have checked the problem.

Manager's Responsibility:

- To pass all requests for Internet access, if authorised, to the ICT department for action.
- If abuse of the Internet is suspected, raise a request to ICT to provide evidence of the abuse. Such a request should only be made if there are sufficient grounds.

Infringement procedure:

If infringement of the above rules is confirmed, the matter should be referred for action under the 'Staff Conduct Procedure', or under the 'Procedure for dealing with Councillor conduct issues'.

Number:	DBC_00025	Title:	Internet Usage Procedure		
Owner:	Info. Security Officer			Last Review	22 nd Jun 2009