

## **INFORMATION FOR STAFF FOR USING THE DEPARTMENT'S ICT NETWORK – Including State School Networks**

### ***Appropriate Use:***

#### ***Why are staff provided access to ICT facilities in the workplace?***

Intranet, internet and network services are important teaching, learning and business tools that can enhance workflow, increase productivity and assist departmental staff to perform a variety of tasks.

#### ***Can a staff member use the departmental network for personal use?***

Staff can use the departmental network for "limited personal use", which means infrequent and brief, generally occurring during personal time and not including: for private business, personal gain or profit; that impede the efficiency of intranet, internet or email services; that would violate or breach any State or Federal legislation and regulation; that would violate or breach the departmental Code of Conduct.

#### ***Does the Department monitor intranet, internet and network usage by staff?***

The Department reserves the right to monitor intranet, internet and network usage and to inspect email messages sent or received by Department officers using ICT resources to:

- Identify inappropriate use: meaning the intranet, internet or network can not be used in a way that defames, harasses, derogates, abuses or offends other intranet, internet or network users, individuals or organisations (for example, to disseminate offensive material based on gender, ethnicity or religious and political beliefs);
- Protect system security;
- Maintain system performance;
- Protect the rights and property of the Department;
- Determine compliance with State and Department policy; and
- Determine compliance with State and Federal legislation and regulation.

#### ***What activities will the Department undertake in monitoring intranet, internet and network services?***

The Department reserves the right to log usage and access of intranet, internet and network services with monitoring and investigation activities undertaken including, but not limited to the following:

- access to and examination of specific types of messages, such as large messages or messages containing executables, audio visual files, movie files, command files and/or pictures;
- access to and examination of messages in specific circumstances, such as at peak periods, where an individual's message volume is high, or on a random sampling basis;
- access to and examination of records for the purpose of complying with investigation requests received from authorities such as Internal Audit, Crime and Misconduct Commission, Freedom of Information, or Senior Management;
- introduction and use of content security software to protect Department officers and the Department's computer network, systems and services from viruses, offensive or libellous material and breaches of confidentiality; and
- conduct a security audit on any privately-owned information technology device used for departmental work purposes (meaning an audit of those sections relevant to the departmental work carried out), where that device is used on departmental premises (e.g. school, District Office, Central Office) and/or is connected to the Department's Wide Area Network (WAN) and a security breach has been detected or the device is suspected to have compromised the integrity of the network.

### ***Inappropriate Use:***

#### ***What action will be taken in relation to violations of departmental policies or misuse of ICT facilities?***

Violations of departmental policies may result in restriction of access to ICT facilities, departmental disciplinary action (including dismissal) and/or action by the relevant regulatory authorities. The State Government's position, described in the Cabinet endorsed [Use of Internet and Electronic Mail Policy and Principles Statement 2007](#) is that "employees may be disciplined or dismissed for the misuse of the internet or electronic mail in respect of material that is offensive or unlawful, although not pornographic. A pattern of behaviour (for example, repeated use) is a factor for consideration in determining disciplinary measures (including dismissal)".

## **Private Device Access:**

### **What to consider when approval has been given to connect a private device to the departmental network?**

While operating private devices connected/connecting to the network:

- maintain availability, confidentiality and integrity of departmental information stored on these devices;
- use these devices in a lawful, responsible and ethical manner; secure passwords; have the required security applications installed before connecting to the departmental or school network;
- maintain the Department's required level and type of security and virus software;
- manage departmental information stored on these devices in accordance with the level of sensitivity (i.e. confidential classifications) for that information;
- back-up departmental information stored on these devices;
- completely remove (not just deleting) all departmental files (e.g. information, software and applications) from these devices (e.g. personal computer, laptop, PDA, diskette, CD): when it is no longer required for departmental work purposes; when officers leave the employment of the Department; before any exchange of equipment under warranty or for repair; or before disposal of the device;
- ensure all software and other material complies with Copyright and Intellectual Property legislation and regulations;
- ensure passwords used to gain access to a private device are not the same as: that used for gaining access to the departmental network; the password used to encrypt/decrypt sensitive folders or files on that device;
- where biometric access control (e.g. fingerprint scanner) is provided on the particular device, this can not be used as the primary method for securing the equipment. Password access, with a suitably strong password, should remain as the initial access control;
- be fully aware that the Department is not responsible for any technical support or upgrade of these devices. Any support or technical advice provided by departmental officers, who will not be held responsible for this advice (e.g. Support Service Desk officers, local system technicians), is sought at the device owner's risk and any subsequent problems encountered are the responsibility of the device owner.
- be fully aware that the Department reserves the right to restrict access of any private device where that device is used on departmental premises (e.g. school, District Office, Central Office) and/or is connected to the Department's Wide Area Network (WAN) and a security breach has been detected or the device is suspected to have compromised/will compromise the integrity of the network.