

# Information Technology Usage Policy

## Authorised Access and Use

Djerriwarrh Community & Education Services (Djerriwarrh) permits the use of the organisation's data communication network through local or internet access by staff, who have valid accounts created that uniquely identify the user.

The organisation's Electronic Communications network is primarily a tool to be used for organisational purposes by participants and staff. This includes communication relevant to:

- Employees and their employment and duties with the organisation;
- Participants and their course activities;
- Participants for job seeking purposes; and,
- Other parties (including contractor or nominated people) for the purpose for which they have been given access to resources.

Electronic Communications must:

- Be used for organisational purposes with limited personal use. Unreasonable or excess personal use will constitute a breach of policy relating to work performance, which subsequently may result in a formal warning or termination (dependant on circumstances);
- Be used like any other organisational communications and must comply with any code of conduct which applies to the user;
- Not be used to conduct private business or private commercial transactions, gamble, or carry out non-work related topics; and,
- Not be used for streaming data such as online games, chat lines, streaming video or studio (film or radio transmissions).

Obtaining unauthorised access to electronic files or emails of others or other unauthorised electronic purposes is not permitted.

Large downloads or transmissions should be minimised to ensure the performance of the electronic communications of other users is not affected adversely.

Djerriwarrh implements a system of different levels of access to information. All employees will be given access to Staff J drive and the drives relevant to their responsibilities and duties.

## Organisation Property

Djerriwarrh is the owner of, and asserts copyright over, all electronic communications created by employees as part of their employment. The organisation reserves the right to re-image its desk tops as and when required.

All web-content that is hosted on the organisation's systems is to comply with the style for content, and will identify the source of the publisher and the date of last update.

The organisation will remove any item that is deemed to be offensive, indecent or

inappropriate. This includes, but is not limited to obscene material, defamatory, fraudulent or deceptive statements, threatening, intimidating or harassing statements, or material that violates the privacy rights or property of others.

Electronic Communications created, sent or received by the users of the organisation network are the property of the organisation, and may be accessed as records of evidence in the case of an investigation. Electronic Communications may also be subject to discovery in litigation and criminal investigations.

### **Monitoring of Information**

Electronic Communications will be used for purposes relevant to the organisation's activities and may be monitored by Authorised People.

The organisation's policy is not to regularly monitor Electronic Communications. However, from time to time Authorised People may examine the records of Electronic Communications for operational, maintenance, compliance, auditing, security or investigative purposes. For example, random monitoring may occur of web sites visited, the contents of email may be required by law to be disclosed or the organisation may investigate a complaint arising from the use of email.

The organisation, under the direction of the CEO, reserves the right to:

- Monitor any device or terminal without notice;
- Inspect without notice, any data or resource owned by the organisation (regardless of ownership), including electronic mail and other forms of communication;
- Capture and inspect any data in networking infrastructure owned by the organisation; and,
- Delete or modify any data in breach of this policy.

The organisation may apply filtering systems to the information systems. The filtering systems may limit the use and activity through:

- Preventing the transmission of email communications - either due to size or content; and,
- Limited access to the World Wide Web and internet sites that are deemed inappropriate and not for the purposes of the core business of the organisation.

Electronic Communications must not be used to send material that defames an individual, organisation, association, company or business. The consequences of a defamatory comment may be severe and give rise to personal and/or organisational liability. Electronic Communications may be easily copied, forwarded, saved, intercepted or archived. The audience of an electronic message may be unexpected and extremely widespread.

### **Infringement of Copyright**

The copyright material of third parties (for example, software, database files, documentation, cartoons, articles, graphic files, text and downloaded information) must not be used without specific authorisation to do so. The ability to forward and distribute electronic messages and attachments greatly increases the risk of copyright infringement. Copying material to a hard disk or removable disk, printing or distributing copyright material by electronic means, may give rise to personal and/or organisational liability, despite the belief that the use of such material was permitted.

The organisation supports the rights of copyright owners and does not and will not tolerate reckless or deliberate copyright infringement.

### **Usage of Electronic Communication and Confidentiality**

Electronic Communication is not a secure means of communication. In the organisation's interest, every attempt is made to ensure the security of the organisation's computer network, users must be aware that this security is not guaranteed, particularly when communicated to an external party. The sender should consider the confidentiality of the material they intend to send when choosing the appropriate means of communication.

Users are required to control the use and release of personal information and restrict access to personal information in order to protect privacy. Collecting, using and disclosing personal information by email may put the privacy of personal information at risk. Personal information and sensitive information should be treated as confidential information. The sender should consider the potential risks of inadvertent or unauthorised disclosure when sending personal information by e-mail. Only the minimum amount of personal information necessary to accomplish the purpose for which it is required should be transferred by e-mail.

The name, Djerriwarrh Community & Education Services should not be used on the Internet for any unauthorised purposes. Any misuse of the organisation's name on the Internet may have a negative impact on the organisation and could subject the sender, management or the Board to legal liability.

### **Computer Viruses**

Electronic Communications are potential delivery systems for computer viruses. Viruses have the potential to seriously damage the organisation's network.

Staff are not to open any downloaded files or emails or attachments that are not expected or look suspicious. In the event that files are received that are suspected of containing a virus, it should be reported immediately to the relevant supervisor/manager, IT site representative or Corporate Services.

Anti virus programs are automatically updated by the IT system.

### **Inappropriate content**

The author and/or the organisation may be liable for what is conveyed in electronic communications. Electronic Communications, whether sent internally or externally, must only contain content that is appropriate to a work place environment.

Electronic Communications must not be used to publish, send or distribute material that is harassing, obscene or threatening, nor may it contain content that may be considered unlawfully discriminatory, offensive or disruptive. This includes sexually orientated messages or images and sexual harassment messages. The receiver of such material will also be in breach of this policy if the communication is forwarded to another email recipient. The receiver should advise the sender to cease sending them. All users of Electronic Communications should be familiar with the organisation's Sexual Harassment Policy.

The use of Electronic Communications for sending 'junk mail', for-profit messages, or chain letters is strictly prohibited.

### **Electronic Communication as Records Management**

Electronic Communications made or received by staff, participants or contractors are public records and subject to the provisions of the Public Records Act 1973.

Email messages that are routine or of a short-term facilitative nature should be deleted when reference ceases, as distinct from ongoing business records such as policy or operational records. Other email messages that are required for the business of the organisation should be printed out and placed on the appropriate files or saved into a folder as appropriate.

Keeping messages fills up large amounts of storage space on the network and can slow down performance. Email accounts should be regularly cleaned up and emails no longer necessary deleted on a monthly basis as a minimum. Incidental personal emails that are not required for organisational purposes should be deleted after reading.

Employee accounts and all data found in the user accounts will be removed from all of the organisation's facilities within one month of the cessation of employment for any reason unless otherwise directed by the CEO.

### **File Attachments**

File attachments in emails can have significant impact on the amount of traffic over the network due to the volume of some of the documents. Senders should carefully consider if an attachment is warranted.

### **Disclaimer**

All E-mails sent externally from the organisation's e-mail service will automatically have a notice attached to them to address electronic legal risks. This notice must not be altered or interfered with in any way, except by Authorised People.

## **Security of Electronic Communication and Systems**

### **1. Staff Passwords**

#### **a) Issuing of passwords**

On commencement of employment, new employees will be issued a Djerriwarrh email address and instructions for accessing the Djerriwarrh IT system. New employees will create their own unique password on their first log in into the system. The systems administrator will generate an access password for each staff member and then the staff member will need to change the access password and enter a new unique password. This may take up to one hour.

#### **b) Security of passwords**

Staff are expected to maintain the security of their password at all times. Passwords must not be written down and left where their purpose is apparent to others. Where a staff member has cause to believe their password is no longer secure they must change their password immediately.

**c) Inactive accounts**

The systems administrator is responsible for monitoring inactive accounts and will investigate the currency of any account which is unused for more than one month. If necessary the account will be cancelled.

**d) Staff Leaving the Organisation**

Any staff member leaving the employ of Djerriwarrh will have their system access revoked on cessation or as directed by the CEO. Line supervisors will notify Corporate Services immediately on the cessation of employees.

**e) Sharing of passwords**

As a general rule no staff member will enable their password(s) to become known by other staff member(s) or external parties.

In the circumstance where a password must be shared to enable business to continue without undue disruption (e.g. through staff absence) this may only be done with the approval of the relevant Manager. The systems administrator must be informed immediately and a new password issued at the earliest practical opportunity.

Where a password has been shared as approved above, the receiving staff member is granted approval to access only the required application(s) and no other information. Any breaches of this approval would be viewed as an unauthorised access of Djerriwarrh systems and subject to disciplinary action.

**2. Unattended machines**

Where a computer is to be left unattended the user **must** sign out or lock the system to reduce the risk of unauthorised usage on the account.

**3. Usage of Memory Sticks / USB flash drives**

**a) Security of data:** Being small and transportable, memory sticks are easy to lose or to leave behind in a remote machine. Staff must ensure that ***all sensitive files*** saved onto a memory stick (or other transportable medium - floppy disk, CD, DVD etc.) are ***password protected*** to protect Djerriwarrh's business information and the privacy of staff and clients' information.

**b) Virus and spyware protection:** As they can be plugged into machines outside of the Djerriwarrh system, the data on memory sticks is ***very susceptible*** to contamination by virus, spyware and related infestations. All staff must ensure that files are scanned for such perils before they are opened or copied into Djerriwarrh's file storage areas.

**c) Original files:** Due to the dangers of loss or damage, Flash drives should only contain copies of files. Original files must be retained within the Djerriwarrh system where they are protected and backed-up regularly.

**d) Responsibility:** It is the responsibility of the user to adhere to the above protocols to protect important and confidential data and the integrity of Djerriwarrh's IT system.

#### **4. Unauthorised Access**

Any unauthorised interception, reading, copying or modifying of electronic data of organisational information technology systems will be in breach of this policy and subject to disciplinary and/or legal proceedings. This will include unauthorised access, modification or deletions of participant records, human resource systems, payroll, financial records, and any other access to organisational electronic systems. It is a breach of this policy to attempt to circumvent the user authentication or security of any host, network or account.

#### **5. Security of Notebook/Laptop Computers**

Where a notebook/laptop computer (whether owned by Djerriwarrh or not) is to be connected to Djerriwarrh's network it is the responsibility of the user to ensure that the machine has up-to-date (<1 month old) virus definitions installed and that the machine has been scanned for viruses and associated security risks. Laptops are to be maintained by the user and any issues notified to an IT site representative in the first instance.

#### **Complaints**

If a user of organisational email or Internet receives an internal or external Electronic Communication that is offensive or inappropriate, it should be raised with the employee's relevant supervisor or manager, or CEO if the manager is the cause of the complaint. Participants should raise the complaint with a staff member or through the Participants Complaints and Appeals Policy.

#### **Policy Awareness**

Staff are made aware of this Policy through:

- (a) Staff induction;
- (b) Regular and timely reminders of the need for compliance with the Policy;
- (c) Providing updates or developments of the Policy; and,
- (d) Establishing a link to the policy upon access to the organisation's IT network.

Participants with access to electronic communications are made aware of this Policy through:

- (a) Providing a copy of the 'The Computer and You';
- (b) Timely reminders of the need for compliance with the Policy; and,
- (c) Discussing relevant sections of the Policy at commencement.

#### **Non-Compliance**

Non-compliance with this Policy will be regarded as a serious matter and appropriate action will be taken when a breach of the policy is identified.

Any failure to abide by this Policy may result in disciplinary action including revoking or restricting any right to use Electronic Communications, cautioning, or, in appropriate circumstances, may lead to more serious disciplinary action in accordance with the organisation's disciplinary policies.

Non-compliance with this Policy may pose a threat to the security of the organisation's network, the privacy of participants, staff and other persons and may expose the users of the system or other persons to legal liability.

A failure to comply by a staff member or contractor will be referred to the CEO, and dealt with in accordance with processes in relation to misconduct or unsatisfactory performance (whichever applicable).

A failure to comply with the Policy by a participant will be dealt with in accordance with the Participant Conduct Policy.

<b>Associated Policies</b>	PO 006 Privacy PO 039 Staff Induction PO 026 Participant Induction PO 003 Sexual Harassment PO 008 Participant Complaints, and Appeals PO 027 Participant Conduct
<b>Associated Procedures</b>	PR 006a Notifiable Data Breach PR 007a Information Technology
<b>Other associated documents Internal</b>	IP 004 Participant Information IP 002 The Computer and You
<b>Relevant Legislation</b>	Public Records Act 1973 Information Privacy Act 2000 Electronic Transactions (Victoria) Act 2000
<b>Other associated documents External</b>	