FEDERAL COURT OF AUSTRALIA

HUMAN RESOURCE MANAGEMENT POLICY

SUBJECT	**Information Technology Policy for Court Employees**
SUMMARY OF POLICY	This policy provides guidance and direction for the use of information technology in the Court and applies to staff, contractors, vendors and others where appropriate.

POLICY NO.	DATE OF ISSUE	DATE OF EFFECT
	February 2012	Immediate

EMPLOYEES AFFECTED	All staff.
CONTACT OFFICER(S)	Director Technology Services Section Director Human Resources
LAST HUMAN RESOURCES POLICY ISSUED (DATE)	N/A
SUPERSEDES POLICY NO.	N/A

1. Purpose

The Court's information technology (IT) resources play a central role in the delivery of the Court's services. This policy provides guidance and direction for their use and applies to staff, contractors, vendors and others where appropriate. The policy is underpinned by three key principles:

- The Court's IT resources must not be used in a way that compromises, or may compromise, the Court's reputation for performing its functions in a fair, impartial and professional manner.
- The Court's IT resources must not be used in a way that may damage or compromise their effective, ongoing operation.
- Where staff make private use of social network sites, non-work Email, internet sites, etc, there must be no inference or implication that the employee represents the Court in any official capacity.

2. Email usage

2.1 Background and Relevant Legislation

Staff sending Email should be aware that all external Email can be identified as originating in the Court and that they have no control over what the recipient does with that mail. Staff should therefore exercise care and judgment in sending Email, particularly with material which:

- Could be interpreted as offensive, discriminatory or constituting harassment.
- Involves confidential or sensitive material.
- May compromise the privacy of third parties.
- May lead to accusations of bias by parties to a matter before the Court.

Email access is provided as a tool to support the Court's official business. Therefore, with the exception of the limited personal use allowed under this policy, the use of Email should be confined to business matters.

The use of both internal and external Email is subject to Commonwealth legislation including the Privacy Act, Archives Act, Freedom of Information Act, the Crimes Act, the Public Service Act and Regulations and the Australian Public Service (APS) Code of Conduct which provides, among other things, that employees must use Commonwealth resources in a proper manner and behave in a way that upholds the APS values and the integrity and good reputation of the APS.

2.2 Security – Internal and External Email

The Court has in place a range of measures to ensure information technology security including user IDs and passwords when first logging onto the network.

Where staff work in open plan work areas, additional security is recommended by locking the workstation when inactive after a defined time. This will stop the unauthorised use of Email accounts when staff are not at their desks.

Other important steps include logging off the Court's network system and turning off the computer when work is concluded each day. Staff who do not connect to the network frequently will automatically receive an update to their anti virus software the next time they connect to the network,

Should the need arise, the Registrar is authorised to view any transaction on the network in order to ensure the integrity of the Court's security, for example, as a result of a reported security breach. This includes Email messages.

Staff using external Email should also be aware of the following points:

- Internet Email is not secure. Staff must not send draft judgments or confidential documents by Internet Email. Staff should seek further advice from Technology Services if a confidential document needs to be sent.
- Documents received from other organisations via external Email are virus scanned automatically upon entering the email gateway.

2.3 Protocols for the use of electronic mail

As noted earlier, all external Email can be identified as originating in the Court and staff have no control over what the recipient does with the message. Staff must therefore use Email in accordance with the following protocols:

- All official communication should be courteous and business-like.
- Messages should be succinct. Attachments should be used for long messages, reports or memoranda.
- Staff are encouraged to include a "signature file" including name, position and contact details for external Email. Signature files can be automatically inserted on all emails if so desired; for assistance in attaching a signature file, contact the Technology Services Service Desk.
- Incidental or occasional personal Email (internal and external) is permitted but excessive, offensive or inappropriate use is a breach of this policy.
- Internal Email may be used on an ad hoc basis to publicise Court social events to staff.
- Staff should exercise judgment when using e-mail on behalf of a third party organisation. While the use of e-mails for school raffles, charity sponsorships, etc, is acceptable, staff are responsible for ensuring there is no potential for a real or perceived conflict or interest, or potential to bring the Court into disrepute. If in doubt, the staff member should discuss with their Director Court Services (or equivalent) in the first instance.
- Email may be used for any business communication where a physical signature is not required.
- Broadcast Email messages should only be sent to judges when it absolutely necessary and appropriate to do so.
- Broadcast Email messages should only be sent to those staff required to receive them and not to a wider audience
- The Email system is not the appropriate medium to use to express criticisms of individuals or to conduct an argument between individuals. Instead these issues should be dealt with via direct contact with the individuals concerned.

- When a staff member is in doubt as to whether a proposed Email usage accords with the Protocol, advice should be sought from their manager.

2.4 Unacceptable use of Email

Staff must NOT send or request material by internal or external Email that:

- Contains illegal, pornographic, abusive or other material which is inappropriate in the workplace and is likely to cause offence;
- Is defamatory. Email messages can be subpoenaed under the Freedom of Information Act 1982, the Privacy Act 1988 and the Audit Act 1901;
- Constitutes a form of harassment or discrimination. Discrimination may occur where any distinction, exclusion or preference is made on the grounds of gender, race, age, medical record, criminal record, impairment, marital status, mental, intellectual or psychiatric disability, nationality, physical disability, sexual preference, religion or trade union activity;
- Contains personal information about another person without that person's consent in circumstances that breach the Privacy Act 1988;
- Copies, re-distributes or otherwise uses another's work in breach of copyright law;
- Constitutes unauthorised software or programs, including games and screensavers;
- Constitutes engaging in illegal activities; or
- Involves gambling.

2.5 'Junk' Email and Spam

The Court has installed a filter (the Barracuda Spam Firewall) to identify and quarantine spam and junk Email. While it is still possible that some spam and junk Email may appear in your Email Inbox, most is removed by the spam filter. Staff also have the ability to classify Email that may look suspicious as spam directly from the Inbox.

Staff should never reply to junk Email or spam or open any attachments as they may expose the Court to viruses as well as further unwanted spam and junk Email. For assistance in managing Email, please contact the Technology Services Service Desk.

2.6 Content Filtering

The Court has implemented software controlled Email content filtering facilities to screen all incoming and outgoing Email traffic. IT Security will use these facilities to quarantine any Email or attachments that represent a potential threat to the security of the network, or contain undesirable content (eg. potential viruses, games, or very large files).

The content of Emails is not read or monitored by TSS staff, other than through the use of automatic software controlled facilities, in accordance with the Telecommunication (Interception) Act 1979.

3. Internet Access

3.1 General

Internet access is provided for official use and should be generally confined to business matters. Web browsing is subject to Commonwealth legislation including the Privacy Act, Archives Act, Freedom of Information Act, the Crimes Act, the Public Service Act and Regulations. The Australian Public Service (APS) Code of Conduct and Values provide that employees must use Commonwealth resources in an appropriate manner and behave in a way that upholds the APS values and the integrity and good reputation of the APS.

3.2 Internet Security

- Contact with all Internet sites passes through the Court's Internet secure 'firewall'. The firewall software scans for computer software viruses and for unauthorised access to the Court's network. Any web pages accessed are automatically virus scanned upon opening.
- In order to ensure the integrity of the Court's security systems, the Registrar can authorise the examination of any transactions on the network that pass through the Court's firewall, including details of websites visited.
- To ensure that no material deemed inappropriate is accessed from the Federal Court network, the Court has implemented an internal system to restrict Internet access to certain categories of sites. A message will notify the user if access to a site in one of these categories is attempted.
- Downloading of applications or programs (eg: any files with the extension "exe") from the Internet is blocked.
- Users are responsible for managing access to their personal computers and particularly for managing their password. Passwords must be complex in nature and should not be provided to any other user. It will be assumed that the user is the person allocated the login and password used.

3.3 Internet Access Protocols

- Incidental or occasional personal use of the Internet that does not interfere with the staff member’s performance of their duties is permitted, but excessive or inappropriate personal use is a breach of this policy.
- Inappropriate use includes accessing material that:
    - Is offensive, derogatory, defamatory or abusive;
    - Is illegal or contrary to policies of the Court;
    - Is sensitive or classified material to which the person does not have approved access;
    - Is discriminatory or constitutes harassment. Discrimination may occur where any distinction, exclusion or preference is made on the grounds of gender, race, age, medical record, criminal record, impairment, marital status, mental, intellectual or psychiatric disability, nationality, physical disability, sexual preference, religion or trade union activity;

- Constitutes personal information about another person, without that person's consent. Such actions may breach the Privacy Act 1988;
- Is a reproduction of another's work where there is reason to believe this is likely to be in breach of copyright law, eg; copies of film or music that can reasonably be assumed to have been downloaded by a third party without legal authority;
- Involves the unauthorised use of software or programs, including games and screensavers;
- Constitutes engaging in illegal activities;
- Involves gambling;
- Contains illegal, pornographic or abusive material or other material which is inappropriate in the workplace and which may or would cause offence to another person.

It is recommended that users exit from the Internet as soon as any task has been completed. Leaving the connection open, when not in use, reduces the speed of the connection for other Court Internet users and may provide the opportunity for unauthorised use by someone else.

Users should also be mindful of the cost, and impacts on the system performance, of downloading audio, video and images from the Internet. Downloading of any such files, as distinct from simply viewing them, should be strictly limited to work related requirements.

It is possible to access offensive and inappropriate material on the Internet quite unintentionally. For example, an appropriate search on the Internet under this policy could result in offensive material being retrieved. It is recommended that, if this occurs, the user log out of the Internet and log back in again, and try an alternative search term. In most instances access to these sites will be blocked automatically.

4. Social Networking and Online Collaboration

Use of Social Networking and Online Collaboration sites, blogs, videoportals or wikis should be done according to the APS Values and Code of Conduct. When using these sites, Court employees are expected to maintain the same high standards that apply elsewhere.

The Court does not block the use of social networking sites such as Facebook, My Space and Twitter. **Incidental or occasional personal use is allowed provided it is consistent with all relevant Court policies, procedures and guidelines and the APS Code of Conduct.**

Social networking sites can, theoretically, be used for official purposes, professional purposes and personal use. This policy relates only to **personal use** of social media.

Court employees may not use social media for official Court purposes unless specifically approved by the Registrar, the Deputy Registrar e-Services, the Executive Director Corporate Services, their District Registrar or the Director Technology Services.

Where staff use social media professionally, for example; as a subject matter expert in their field, there is a strong potential for this to be identified directly or indirectly with

the Court. Staff are therefore required to advise the Registrar should they wish to use social media for this purpose.

Staff using social networking sites must not mix the professional and personal in ways that may bring the Court into disrepute or raise issues of real or perceived (apprehended) bias or conflict of interest. Chambers staff particularly should consider the potential for issues of apprehended bias and staff should bear in mind the APS Code of Conduct requirements to:

- Disclose, and take reasonable steps to avoid, any conflict of interest (real or apparent) in connection with Court and APS employment.
- At all times behave in a way that upholds the APS Values and the integrity and good reputation of the Court and APS.
- Use Commonwealth resources in a proper manner.
- At all times behave in a way that upholds the APS Values and the integrity and good reputation of the APS.

4.1 Private use of social networking and Online Collaboration

Staff should avoid identifying themselves as Federal Court employees on their private social networking sites and avoid posting material to a site that identifies or relates to their employment. Personal use of these sites must be associated with a personal email address and Court email addresses must not be used.

Staff should also be aware that, whether or not they are identified as Court employees, other staff and clients of the Court may access the site and may raise issues where they believe there is a possible conflict of interest or the integrity or reputation of the Court may be compromised. For example, adding a client or Court user as a 'friend' may raise questions of bias in the eyes of others, depending on the role of the staff member.

Similarly, a person who can be identified as an APS or Court employee who posts offensive, racist or obscene material – even on their own time and using their own resources – could be in breach of the Code of Conduct in much the same way as a person shouting offensive, racist or obscene comments in a public place. Practical steps that may assist include:

- Checking your account and privacy settings
- Reviewing your posts before adding them to your site/profile
- Considering 'friend' requests carefully and monitoring material 'friends' may post on your site

While the Court recognises the right of staff to privacy and as clear a demarcation as practicable between their work and private lives having regard to the nature of their job, staff should also be aware that social networking sites have the potential to raise issues that did not arise with earlier technology. If in doubt, staff should feel free to discuss any concerns with their District Registrar or Director Court Services.

4.2 Blogs and posting comments online

As with other social networking sites, staff should avoid identifying themselves as Federal Court employees when posting comments or participating in on-line discussion unless prior approval has been obtained from the Registrar, the Deputy Registrar e-Services, the Executive Director Corporate Services or their District Registrar.

Similarly, whether or not staff are identified as Court employees, other staff and clients may access the site and may raise issues where they believe there is a possible conflict of interest or the integrity or reputation of the Court may be compromised. Staff are therefore required to apply the standards and principles applying to the use of social media and networking sites when posting comments on line.

5. Failure to comply with this policy

The Court's reputation and the integrity of its IT facilities relies on those using the Court's IT facilities doing so in accordance with this policy.

Failure by an employee to comply with this policy will be regarded as a serious matter and may lead to formal misconduct proceedings which could result in a range of sanctions, including dismissal.

More generally, a breach of this policy by any user of the Court's IT facilities may also entail a breach of other legislation including the Crimes Act and anti-discrimination legislation and may lead to action under that legislation.

6. Questions

General queries on the Court's IT facilities can be referred to the Technology Services Service Desk.

Security-related questions should be directed to the IT Security Manager