Procedure 5.09.1 Internet, Intranet and email acceptable use

<table>
<thead>
<tr>
<th>Department</th>
<th>Strategy &amp; Business Services</th>
</tr>
</thead>
<tbody>
<tr>
<td>Responsible Officer</td>
<td>Manager</td>
</tr>
</tbody>
</table>

Introduction

E-Mail and Internet opens up many opportunities, but it also presents many threats. The purpose of this policy is to obtain the best value from this technology at the lowest acceptable risk.

Definitions

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Virus software</td>
<td>Anti-Virus software is an application that runs on all of Council’s computers. It is one of the tools used by Information &amp; Communication Technology (ICT) section in ensuring the integrity of Councils network and data. The term Virus Software is not limited to mean any specific application, but may from time to time include other brands and styles of protection as deemed necessary by the ICT department.</td>
</tr>
<tr>
<td>Security</td>
<td>The Internet and e-mails should be regarded as an inherently insecure environment. Confidential information should not be transmitted via these mediums. No personal information should be transmitted without the consent of the individuals concerned. Refer to Procedure 5.09.5 Information security</td>
</tr>
<tr>
<td>Abuse of internet and e-mail access</td>
<td>Any user who is deemed by the General Manager to have abused the use of the Internet or e-mail will have access to the Internet removed and may be subject to disciplinary proceedings.</td>
</tr>
<tr>
<td>Interfering with virus protection</td>
<td>Any user who is deemed by the General Manager to have interfered with Virus Software in any way, which exposes Council’s network and data, will have access to the Internet and e-mail removed and may be subject to disciplinary proceedings.</td>
</tr>
</tbody>
</table>

General principles

1. Council provided Internet/Intranet and e-mail privileges, like Council computer systems and networks, are considered Council resources and are intended to be used for business purposes only. Usage and content may be monitored for unusual activity.
2. Correspondence via e-mail is not guaranteed to be private. Confidential e-mails should not be sent without encryption.
3. Council e-mail accounts, Internet IDs and Web pages should not be used for anything other than Council-sanctioned communications.
4. Use of Internet/Intranet and e-mail resources may be subject to monitoring for security and/or network management reasons.
5. The distribution of any information through the Internet, computer-based services, e-mail and messaging systems is subject to the scrutiny of Council management. Council reserves the right to determine the suitability of this information.
6. Internet usage must be able to survive public scrutiny and/or disclosure. Users must avoid accessing sites that may bring the Council into disrepute, such as those, which carry offensive material. Sensitive information must not be transmitted via or exposed to Internet access.

7. Employees may use Internet services for personal improvement, outside of scheduled hours of work, provided that such use is consistent with professional conduct and is not used for personal financial gain.

8. Internet forums such as newsgroups may be used only to conduct work related business or to exchange technical or analytical information. Users who wish to express personal opinions must use a private Internet provider and a personal ID.

9. Internet forums such as Social Networking sites and Blogs is limited to approved users refer to Procedure 5.09.4 Social Media.

10. The ICT section must ensure that all users sign an Internet Usage Agreement (attached) before access is allowed. This agreement may be incorporated into existing system access agreements.

11. The ICT section monitors the use of the Council network. Information incoming and outgoing via the Internet or E-mail will be scrutinised at any time by the ICT section under delegated authority from General Manager. Alleged inappropriate use of the Internet will be reviewed by the ICT Manager on a case by case basis and referred to the appropriate Manager for disciplinary action to be taken in accordance with the policy, up to and including dismissal or cancellation of contract.

12. All e-mail messages are archived, and could be viewed by authorised personnel under delegated authority from General Manager at any time.

13. All e-mail messages are scanned for viruses, and if deemed suspicious will be quarantined at the email gateway.

Responsibilities

1. Users are required to complete and sign a copy of the Internet, Intranet and E-mail usage declaration form at commencement of their employment with Council. The appropriate Human Resources officer will provide staff with this document upon commencement.

2. Users are responsible for ensuring that their use of Internet and e-mail access is appropriate and consistent with ethical conduct under this procedure and with policy 5.02 Behaviour of Councillors and Staff.

3. The ICT section is responsible for ensuring that all employees who have Internet access have signed an Internet Usage Agreement and that it is placed in the employee's personnel file, and that computers used to access the Internet and e-mail have approved anti-virus software.

4. Managers, Supervisors and ICT staff are responsible for reporting instances of contravention to this procedure to the Workforce and Administration section, which will ensure that the appropriate disciplinary action according to this procedure is taken.

5. Staff are required to read and ensure that they understand any correspondence from the ICT section with regard to Virus Warnings. If any staff are in need of clarification of any correspondence they are to contact ICT before further utilising any computer software or hardware.

6. Emails are considered correspondence under the State Record Act and as such it is the responsibility of the individual to ensure that w copies of email received are registered in Council Electronic Document Management System for retention.

7. As a general rule any e-mail containing attachments should be considered suspicious. If in doubt ICT should be contacted before accessing, opening, replying or forwarding of any suspicious e-mail.

Web browsing

All Web browsing is to be for an organisational need and usage will be monitored to ensure that this is followed. File downloading is permitted, with the exception of application and operating system files. The files are to be downloaded to the appropriate directory. The use of and access to “streaming” Internet sites is not allowed.
These sites may include, radio stations, media sites, music sites (video or audio), film/movie/mpg sites and sports relay sites.

Web publishing

Council’s in-house "Web Administrator" will deal with publishing on the Web where final recommendations for material to be included will be made.

Social Networking Sites

Access to social networking sites is limited to approved users (refer to Procedure 5.09.4 Social Media).

Conditions of use

Users shall NOT:

1. Breach any applicable laws and regulations and must respect the legal protection provided by copyright and licenses with respect to both programs and data.
2. Use Council’s Internet to visit Internet sites that contain obscene, hateful or other objectionable materials; send or receive any material that is obscene or defamatory or which is intended to annoy, harass or intimidate another person.
3. Use Council’s Internet or e-mail for the purpose of gambling.
4. Solicit e-mails that are unrelated to business activities.
5. Solicit non-Council business for personal gain or profit.
6. Use Council’s Internet or e-mail for any illegal purpose.
7. Attempt to obscure the origin of any message or download material under an assumed Internet address.
8. Represent personal opinions as those of Bega Valley Shire Council.
9. Make or post indecent remarks, proposals, or materials.
10. Upload, download, or otherwise transmit commercial or any other executable software or any copyrighted materials belonging to parties outside of Council, or to Council itself.
11. Download any software or electronic files without ensuring compliance with Council’s approved virus protection measures and procedures.
12. Intentionally interfere with the normal operation of the network, including by the propagation of computer viruses and sustained high volume network traffic, which substantially hinders others in their use of the network.
13. Reveal or publicise confidential or proprietary information which includes, but is not limited to:
   a. financial information;
   b. Council business, strategies, plans, databases and the information contained therein;
   c. client, ratepayer, resident or other community information;
   d. technical information;
   e. computer/network access codes; and
   f. information about Council’s business relationships which they are not authorised to release, reveal or publicise.
14. Examine, change or use another person’s files, output or user name for which they do not have explicit authorisation.
15. Perform any other inappropriate activities or uses identified by the network administrator.
17. Remove, disable, modify or interfere with in any way Virus Software loaded on any Council computer unless under direct instruction by the ICT section.
Sanctions

Users who violate any of the conditions of this policy may be subject to disciplinary action including (but not limited to) written warnings and revocation of access privileges. Council also retains the right to report any illegal violations to the appropriate authorities.

Other relevant documents

This procedure is to be read in conjunction with policies 5.09 Information Technology and 5.02 Behaviour of Councillors and Staff. It is also to be read in conjunction with procedures 5.09.3 Computer hardware & software acceptable use, procedure 5.09.5 Information security, procedure 5.09.4 Social Media, Procedure 5.09.6 and procedure Accessing Council information via “BYOD” (Bring your own Device).
I, (print name) ______________________________ acknowledge that I am being granted Internet and e-mail access using Council facilities in order to carry out my work and agree that my use of the Internet will be conducted in an ethical and professional manner.

I agree that I will not use this access for personal use during scheduled hours of work. I also agree that personal use will not include inappropriate behaviour such as access to or downloading from offensive sites; personal (non-work related) or activities for personal financial gain.

I understand that I have been given notice in accordance with section 10(2) of the Workplace Surveillance Act 2005 (NSW); and that Council will be entitled to, and shall commence monitoring, all my personal and business use of these services and communication facilities, and that monitoring will be in accordance with this policy and that inappropriate usage may be cause for disciplinary action up to (but not limited to) written warnings and revocation of access privileges.

I understand that my use of the Internet and e-mail is identifiable by others as a Council activity and acknowledge that it is my responsibility to ensure that my usage does not contravene any laws or regulations, including copyright and licensing issues and laws respecting obscene and discriminatory material. I agree that I will not transmit sensitive material via the Internet or e-mail.

I understand that if I am not prepared to accept any of these conditions of this policy that access to e-mail and internet facilities will NOT be granted.

I understand that by signing this document that I acknowledge that I have read and understood this document. I further understand that it is my responsibility to seek advice regarding any questions that I might have regarding this document prior to my signing.

Signed ______________________________ Date ____________________________
Witness name ______________________________ Witness signature ____________________________