Preamble

This policy is established to employees guidance on the standards and expectations Bega Garnbirringu Health Services (Bega) maintains in regards to the use of Computers, Internet and email within the organisation. This policy is to be read an applied in conjunction with the organisation's Social Media Policy. No policy can lay down rules to cover every possible situation. Instead, it is designed to express the organisation express intent to set forth general principles when using computers, email, and internet whilst at work, or whilst using Bega devices.

Policy Statement

This policy also outlines the parameters and proper, approved use of Bega's internet connection, email, computer and network systems as used by its employees and contractors. It covers the use of the World Wide Web and associated services of internet browsing etc., as well as the approved and intended use of computers (including but not limited to devices such as laptops, mobile phones and smartphones), provided by the organisation to its employees.

This policy statement covers all communication via email, Internet or social media. Where that communication is made by an employee of Bega. It applies at all times across the entire organisation, despite whether it is used on a personal or work device or computer.

Communication covered in this policy relates to:

- The use of Bega's company name;
- Internal business matters including documents and intellectual property of Bega;
- Any confidential business or client related information;
- Information that is, or could be seen as, threatening, defamatory, racist, discriminatory, intimidating, harassing, vilifying or a vexatious or harmful nature or intent;
- Information that in any way breaches or compromises Bega's Code of Conduct;
- Publicises comments on workplace matters, political or religious viewpoints.

Policy Guidelines

EMAILS

The content of an email message is essentially considered a letter on company stationery by the recipients. Therefore, email communication should follow the same standards expected in written business communications and public meetings. Email and web browsing are not guaranteed to be treated as private records of the employee. *The organisation has the right to monitor, review and retrieve emails on request and access web browsing records.*

Email is a tool for business communication and employees have the responsibility to use this resource in an efficient, effective, professional and lawful manner.

The organisation retains logs, backups and archives of computing activities, which it audits from time to time.

These records are the sole property of the organisation and are subject to State and Federal compliance laws and may be used as evidence in legal proceedings, or in workplace investigations into suspected misconduct.

Employees must not alter the approved email signature that is attached to every email sent out by employees. The disclaimer and branding of the organisation as presented in the email signature template and is approved by the Chief Executive Officer.

Bega may choose to use and disclose the Computer Surveillance records of any employee (see more information below on Surveillance) where that use is:

- for a purpose related to the employment of any employee or related to Bega business functions;
- to a law enforcement agency in connection with an offence;
- in connection with legal proceedings.

For example, use or disclosure of Computer Surveillance records can occur in circumstances of assault, suspected assault, theft or suspected theft of the Bega property.

All email sent and received by the organisation's email system is automatically filtered by protective software. The following Internet message types will be automatically quarantined and deleted by the message filtering software and may be reviewed:

- Messages that contain large amounts of non-business information;
- Messages with offensive, sexual, racist or profane language;
- Unsolicited junk email; and
- Virus or Malware infected email.

The following are **prohibited** activities when using email. The creation and exchange of messages that:

- Are offensive (including swearing and profanity), harassing, vulgar, obscene, threatening or defamatory. This includes text, images, sound or any other material, sent either in an email or in an attachment to an email, or through a link to a site (URL);
- Information that could insult, offend, intimidate or humiliate
- Is illegal, unlawful or inappropriate;
- Gives the impression of, or is representing, giving opinions or making statements on behalf of the organisation without the express authority of the Chief Executive Officer. Further, employees must not transmit or send any documents or emails (in any format) to any external parties or organisations unless expressly authorised to do so and/or is in their scope of job duties;
- The exchange of proprietary information, trade secrets or any other privileged, confidential or sensitive information or information subject to privacy obligations (subject also to the organisation's policy on confidentiality and privacy);
- The creation and exchange of advertisements, solicitations, chain letters and other unsolicited email;
- Registration to email subscriptions without authorisation from the employee's Manager;
- Use of auto-forwarding rules to unauthorised external email addresses;
- Use of email which disrupts the network or other users;
- Use of email for personal commercial activities, whatever the frequency of use or size of the email;
- Using the email to send all staff messages that are not business related; and
- Messages being read or sent from another user's account except under agreed delegated arrangements.

Acceptable email use includes:

- Email is provided to employees primarily for business purposes and personal use should be kept to a minimum. Users are reminded that as per the conditions of the *Criminal Code Act 1913* copies of all emails sent and received are archived and may be monitored for misuse;
- While it is acknowledged that employees cannot always control the email they receive, employees are obliged not to forward any 'unacceptable' email, even if you believe the recipient would not find the material offensive;
- Provide a copy of *all staff* emails to your Manager for distribution; and
- Employees also have an obligation to review email and to immediately delete unacceptable email from the system. You should also notify your Manager and request to be removed from inappropriate distribution lists if this does occur.
- Employees should make every effort to ensure the confidentiality of electronic messages is appropriately maintained in accord with the organisation's confidentiality policies. Employees should therefore forward confidential electronic messages to other recipients only if there is an organisational need, and with the approval of the original sender, where possible;
- If an employee receives an email which the employee suspects contains a virus, the employee should not open the email or attachment to the email and should immediately contact the Information and Communication Technology (ICT) department for assistance;
- If an employee receives an email the content of which (including an image, text, materials or software) is in breach of this policy, the employee should immediately delete the email and report the matter to their Manager. The employee must not forward the email to any other person.

Other considerations for emails use:

- Email records shall have the same retention periods as records in other formats that are related to the same program function or activity;
- Email records must be retained in the system for as long as it is required to meet record keeping requirements, and must be readily accessible to meet business and legal requirements;
- Email records must be maintained in such a way as to ensure that the email record is authentic, accessible and comprehensible for as long as it is required to be retained;
- Access Controls should be implemented to prevent the disclosure of retained email to unauthorised personnel as managed by the Executive Management;
- Email records reasonably likely to be required in evidence must not be destroyed; and
- Where an employee is uncertain about the appropriate use of emails, they should discuss this with their Manager.

INTERNET

Bega's Internet connection provides authorised staff and contractors with access to the vast amount of information available. This policy has been formulated to deal with issues related to legal liabilities, network bandwidth and employee productivity.

Use of the Internet by employees is permitted and encouraged by authorised users where such use is suitable for ***only*** operational purposes and supports the mission and objectives of the organisation. The Internet is to be used in a manner that is consistent with professional standards.

The following use of the Internet is **NOT** allowed:

- Accessing the Internet via another users account;
- Viewing, downloading or distributing offensive or illegal material, including but not limited to copyright material, pornography, nudity, hate or discrimination related media etc.
- Use, which causes disruption to the network or other users (e.g. excessively large downloads or streaming media);
- Use for personal, including commercial activities;
- Connecting the organisation computers to the Internet via means other than approved connections;
- Using network passwords on external web sites; and
- Blogs, Social Media Networks and sites not operated by the organisation.

Employees have the right to contribute their own personal content to public communications on websites not operated by organisation, such as social networking sites like Facebook or Instagram. Refer to the organisation's Social Media policy for more information on using these platforms. However, any inappropriate and/or extended use of such communications has the potential to cause damage to the organisation's operations

If it comes to the organisation's attention that an employee has made inappropriate and/or unauthorised comments about Bega, its employees, clients or Board Members, the employee will face disciplinary action.

NETWORK

Employees who use a Bega provided device include phones, laptops, computers, dongles, iPads, and/or other electronic devices must at all times:

- Handle the equipment in a responsible manner and ensure that the equipment is kept secure;
- Use their own username/login code and/or password when accessing the network;
- Protect their username/login code and password information at all times and not divulge such information to any other person, unless it is necessary to do so for legitimate business reasons; and
- Ensure that when not in use or unattended, the Computer System is logged off, locked or shut down, before leaving their workstation or device.

Employees must not use the organisation's computer Network:

- In a manner contrary to the other organisational policies;
- To create any legal or contractual obligations on behalf of the organisation;
- To install software or run unknown or unapproved programs on the organisation's Network; and
- To gain unauthorised access (hacking) into any other computer within the Network.

SURVEILLANCE

On a continuous and ongoing basis Bega may carry out computer surveillance to ensure that email, internet and the computer network are being used in compliance with this policy.

Computer Surveillance occurs in relation to:

- storage and download volumes;

- internet sites - web sites visited is recorded including the time of access, volume downloaded and the duration of access;
- malware or viruses;
- emails - the content of all emails received, sent and stored on the Computer Network. This also includes emails deleted from the Inbox; and
- computer hard drives – all local drives are backed up on the Bega computer network, so the storage of personal information or records is not recommended.

Bega retains logs, backups and archives of all computing activities on our network including emails, website usage and social media access, which it audits from time to time. Such records are subject to State and Federal laws and may be used as evidence in legal proceedings, or in workplace investigations into suspected misconduct.

Breach of Policy

If an employee does not meet the expectations set out in this policy, they may be subject to disciplinary action in accordance with the organisation's **Performance Counselling** and **Disciplinary** policies up to and including possible termination of their employment.

Related Documents

- Privacy Policy;
- Confidentiality Policy;
- Bega Code of Conduct;
- Social Media Policy.