GELOS
ENTERPRISES

Digital Communications Policy and Procedure

Contents

1. About this policy and procedure

1.1 Document purpose

The purpose of this Digital Communications Policy is to provide guidelines for all Gelos staff for creating, sending, receiving, and using professional digital communications that reflect an attitude of excellence.

1.2 Scope

All staff must comply with this policy in their conduct of official business for Gelos Enterprises. This policy reflects the responsibilities of Gelos and individuals as outlined in the following legislation:

- Privacy Act 1988 (Cth)
- Privacy Fact Sheet 17: Australian Privacy Principles
- Privacy and Personal Information Protection Act 1998 (NSW)
- Workplace Surveillance Act 2005 (NSW)

This policy has been authorised by the Managing Director and is available to all staff. It has been developed in consultation with staff and will be revised on a regular basis.

2. Policy

Gelos is committed to producing professional digital communications that reflect an attitude of excellence. This Digital Communications Policy exists to outline the key principles and procedures when creating, sending, and receiving communications sent by email, mobile phone, instant messaging, and within online meetings.

Be aware that digital communications could be forwarded, intercepted, printed, and stored by others. Staff also need to be mindful of Privacy Legislation and are accountable for digital communications sent in their names or held in their mailbox. You should use digital communications ethically and properly.

All digital communications should:

- be professional and use a positive and polite tone
- follow the guidelines relating to the transmitting of sensitive or controversial information
- be clear, concise, correct, and courteous
- use appropriate punctuation, grammar, and spelling
- use Gelos' templates and style guide
- be reviewed and proofread before sending
- not use obscene, profane, lewd, vulgar, rude, inflammatory, or threatening language in public or private messages
- not include information that could cause damage to property or persons if acted upon
- not include deliberately false or defamatory information about a person or organisation
- not engage in personal attacks including prejudicial or discriminatory attacks or harass another person
- be used to conduct the business of Gelos. Keep digital communications of a personal nature to a minimum.

3. Digital Communications Procedure

3.1 Security

- Passwords should be kept confidential and not shared with others. They should be changed and determined per the Information Security Policy requirements.
- Keep all computers, mobile phones, and other devices secure and take reasonable measures to safeguard the physical devices from theft or damage.
- Do not use or download unauthorised programs, software, graphics, or music that is not associated with the conduct of Gelos' business.
- Do not use Gelos digital communication services to send inappropriate messages including email chain, spam, or hoax messages.
- Allow anti-virus software to scan, prevent and protect digital messaging from malware, viruses, and phishing messages.

3.2 Ethical Behavior

- When using Gelos digital communication services, always follow the Gelos' Code of Conduct and principles of communication etiquette.
- Do not use Gelos digital communication services for unauthorised commercial or illegal activities, online gaming or gambling activities.
- Do not use Gelos digital communication services to access material that is profane, obscene, pornographic, and paedophilic, promotes illegal acts, or advocates violence or discrimination.
- Avoid the use of jokes and sarcastic comments.
- Do not send intimidating, hostile, or offensive material, including images, videos, or text which someone may be view as indecent, pornographic, obscene, illegal, discriminatory, offensive, or abusive.

- Do not send material that may be threatening, bullying, or harassing to another person or include knowingly false or defamatory information about a person or organisation.
- All policies and procedures for dealing with discrimination, harassment, intimidation, and abuse in the workplace also apply when collaborating online with others as part of your work role.

3.3 Privacy and Confidentiality

- Never publish or disclose another person or user's email address or personal information without that person's explicit permission.
- Mark all confidential information as 'confidential' and disposed of properly. Do not leave confidential information visible on devices such as computer monitors and tablets when you leave them.
- Avoid using digital communications to transmit commercially sensitive information.
- If using digital communications to transmit commercially sensitive information, double-check you have included the correct recipients and email addresses.
- Do not attempt to gain unauthorised access to Gelos information assets and digital services.

3.4 Suspicious emails and messages

- Report all suspicious emails to the ICT Helpdesk and your supervisor. Once reported, delete the email and block the sender. Do not forward or reply to the email or click on any links in the email.
- Report any actual or suspected security violations, breaches, weaknesses and vulnerabilities to the Gelos ICT Helpdesk.
- Promptly inform Gelos ICT Helpdesk if you suspect you have received a message that is inappropriate or may have malware or virus infection.

- Do not knowingly send or forward messages including computer malware, malicious attachments, or links that are capable of damaging recipients' computers.
- Set all security levels and filters for incoming digital communications as outlined in the Information Security Policy.

3.5 Email

- All emails should follow the Gelos email template, including style guidelines, email signatures, and confidentiality disclaimer.
- All emails should use appropriate punctuation and grammar. Before sending, all emails should be spell checked, proofread, and recipient email addresses checked.
- If an email is returned, check the addressee's email address with another source. If correct, contact the recipient by phone. If the addressee's email is incorrect, resend the email.
- Review email inboxes regularly and file emails in relevant Gelos department folders. Emails should be deleted or archived per the Electronic Records Management Policy.
- When receiving an email, determine its urgency and confidentiality. You should reply to emails within one business day.
- When sending an email, identify if your message is urgent.
- Email attachments should not exceed 2GB due to server requirements.

3.6 Instant Messaging

- Instant messages should not include confidential, personal, non-public, or commercially sensitive information.
- Do not use instant messaging for communications to be retained under the Electronic Records Management Policy.

- Do not use instant messaging to share personal views on social, political, religious, or other non-business related matters or send unsolicited commercial or advertising content.
- Do not use instant messaging for excessive personal use that interferes with the team's work duties or performance.
- Report any communications with inappropriate content to your supervisor.
- Your Instant Messaging status should be accurate. It should not show as offline, busy, or in a meeting if you are available. The instant messaging application should be open during your working hours. You should respect the status of others when sending messages.

3.7 Mobile phones

Gelos may provide team members with a Gelos mobile phone to contact other Gelos employees, customers, suppliers, and stakeholders. The following procedures apply to these mobile phones:

- Use mobile phones carefully, ethically, effectively, and efficiently.
- Minimise private use.
- Mobile phones include a Find My Phone application. Keep location services turned on at all times.
- Keep mobile phones turned on during working hours. They should be turned on silent when in meetings.
- Set up voicemail for unanswered calls. Respond to voicemail messages within three business hours. The voicemail message should be short and professional. For example, 'Hello, this is (your name), (position) of Gelos. I am unable to take your call right now. Please leave your name, number, and a short message after the tone. I will return your call shortly.
- Voicemail should be updated if you are on leave or unavailable for more than one business day.
- Lost, stolen, or damaged phones should be reported to the ICT Helpdesk and your supervisor as soon as possible.

Private use of personal mobile phones during business hours should not interfere with your or your team's normal work duties or performance. Keep personal mobile phones on silent.

The following applies to all mobile phones, both provided by Gelos and personal mobile phones:

- Do not use mobile phones while operating a motor vehicle unless a 'Hands-free Car Kit' is installed in your vehicle and permitted by law.
- Do not use mobile phones in a manner that creates unsafe or potentially unsafe situations or an actual or potential work health and safety risk.

3.8 Online meetings

- Hold all online meetings using Microsoft Teams.
- Gelos' employees should use their Gelos Microsoft Teams account and the provided headset to participate in meetings.
- It is expected all participants arrive on time, prepared for the meeting.
- Backgrounds should use the blurred background feature.
- Cameras should not show any intimidating, hostile, or offensive material, including images, videos, or text which may be viewed as indecent, pornographic, obscene, illegal, discriminatory, offensive, or abusive.
- Tell all participants if an online meeting is being recorded. Do not record if a participant objects.
- Do not send recordings to people outside of Gelos.

4. Document information and review

4.1 Responsibilities

The following staff members have key responsibilities in implementing this policy and procedures.

The Managing Director is ultimately responsible for the effective implementation of this policy and procedures in Gelos.

The Head of ICT will oversee the formal monitoring of this Digital Communications Policy and appropriate use of devices. However, it is the responsibility of all staff to monitor their behaviour and performance and alert their supervisor and ICT Helpdesk to any concerns.

The Head of ICT is responsible for providing advice and support on Digital Communications Policy and procedural matters. If you are asked to do something that breaches this Digital Communications Policy or have any concerns, please talk directly to the Head of ICT.

All team members are responsible for adhering to this policy and associated procedures.

Gelos' management's responsibility is to ensure this policy is effectively communicated, understood, and implemented throughout all business operations.

Table 1 – Responsibilities

Staff member	Responsibilities
Head of ICT	Endorse the Digital Communications Policy and procedure Comply with the Digital Communications Policy and procedure
Management team	Monitor teams' compliance with the Digital Communications Policy and procedure Comply with the Digital Communications Policy and procedure
Staff member	Comply with the Digital Communications Policy and procedure

4.2 Definitions

The following definitions clarify the terms and words that are specific to this policy and procedure.

Table 2 – Definitions

Term	Definition
Commercially sensitive information	Information that could have actual or potential value or impact on the commercial operations of the organisation. If disclosed, commercially sensitive information could place Gelos at a disadvantage or impact its commercial interests. Examples include operational data, work obligations; revenue and cash flow data; and employee information.
Confidentiality	Confidentiality applies to the relationship of confidence. Confidentiality ensures that information is accessible only to those authorised to have access. Confidential information may be marked as such or deemed confidential by its nature.
Confidential information	Information disclosed, provided, or otherwise made available during an employee's period of employment; work they have contributed to or made in the course of their employment, which may include but is not limited to the business and affairs of Gelos. Confidential information does not include information that is considered public knowledge at the commencement of employment with Gelos or information that became so at a later date. Confidential information must only be used in the course of employment and may not be released or taken offsite without authorisation from an employee's line manager.
Digital services	A service delivered via the internet or an electronic network. Supply is essentially automated or involves only minimal human intervention.
Information asset	A body of information, defined and managed as a single unit so it can be understood, shared, protected, and exploited efficiently. Information assets may be physical or electronic.
Non-public information	Information specific to the organisation and not considered to be public knowledge.

Personal information	Information or an opinion about an identified or reasonably identified individual.
Public domain	The public domain in relation to confidentiality is common knowledge. That is, information that can be accessed by the public.

4.3 Related documents

This policy and procedure should be read in conjunction with the following documents:

- Code of Conduct
- Confidentiality and Privacy Policy
- Electronic Records Management Policy
- ICT Quality Management Policy
- Information Management Policy
- Information Security Policy
- Social Media Policy

4.4 Document review

This policy and procedure will be reviewed every 12 months.

Review date: [Click/tap to enter a date]

4.5 Document authority

This Digital Communications Policy and Procedure has been authorised by Catherine Dunn the CEO of Gelos Enterprises and is available to all staff. It has been developed in line with all relevant legislation, in consultation with committee representatives and will be revised on a regular basis.

Approval date: [Click/tap to enter a date]