Corporate Email Usage Policy

1. Policy brief & purpose

Girl Guides South Australia (**GGSA**) recognises that staff and volunteers require access to email and other IT systems to assist in the efficient and professional delivery of services.

Our corporate email usage policy provides direction to support staff and volunteers use their company email addresses appropriately. Email is essential to our roles. We want to ensure that our staff and volunteers understand the limitations of using their corporate email accounts.

Our goal is to comply with current legislation, protect our confidential data from breaches, and safeguard our reputation and technological property.

2. Scope

This policy applies to all staff and volunteers who are assigned or given access to corporate email. This email may be assigned to an individual (e.g. name@girlguidessa.org.au), a role (e.g. chair@girlguidessa.org.au) or unit (e.g. unit@girlguidessa.org.au).

3. Policy elements

Corporate emails are powerful tools that help staff and volunteers undertake their roles. Staff and volunteers should use their corporate email only for Girl Guides South Australia Inc. related purposes.

This policy defines what constitutes appropriate and inappropriate use. Staff and volunteers must always adhere to this policy, in addition to complying with any Confidentiality Agreements, other relevant GGSA or Girl Guides Australia policies.

i. Inappropriate use of a corporate email

GGSA staff and volunteers represent GGSA whenever they use their corporate email address. They must **not**:

- Sign up for or access:
  - Illegal, unreliable, disreputable, or suspect websites and services
  - Copyrighted information in a way that violates the copyright.
  - Websites containing inappropriate (including pornographic) or criminal material.
  - Internet-enabled activities such as gambling, gaming, conducting a business or conducting illegal activities.
  - Download eBooks, guides, and other content for their personal use.

- Send:
  - Unauthorised marketing content, solicitation emails or bulk emails
  - Spam to other people's emails, including other staff or volunteers.
  - Chain letters.
  - Company confidential messages to external locations unless necessary to carry out the business of Guiding.
  - Unsolicited personal views on social, political, religious, or other non-Guiding related matters.

Dated: August 2024
Review August 2026

  - Messages that are offensive, harassing, obscene or threatening.
  - Confidential or sensitive information held by Girl Guides South Australia (unless within the authorised course of their duties).

- Carry out:
  - A personal business.
  - Non-Guiding business.

- Distribute, disseminate, or store images, text or materials that might be considered indecent, pornographic, obscene, or illegal.

- Intentionally introduce any form of computer virus or malware into the corporate network.

ii. Appropriate use of corporate email

Staff and volunteers should use their corporate email for all work or Guiding related purposes. For example, staff and volunteers should use their email to:

- Communicate with current or prospective Girl Guides and parents or carers of Girl Guides, other staff and volunteers, and corporate partners and stakeholders.
- Provide their email address to people they meet at networking events, professional forums, and other corporate events for business or Guiding purposes.
- Sign up for newsletters, platforms and other online services that will help them with their roles or professional growth.
- Email accounts may be shared only, when necessary, by leaders within a particular unit or for those in shared roles.

iii. Personal use

Staff and volunteers may have a need from time-to-time to use their GGSA email for personal reasons. Limited personal use is permitted where it:

- Is infrequent and brief.
- Does not interfere with the duties of the staff and volunteers or his/her colleagues.
- Does not interfere with the operation of Girl Guides South Australia.
- Does not compromise the security of the Girl Guides South Australia systems.
- Does not impact on Girl Guides South Australia's electronic storage capacity.
- Does not decrease Girl Guides South Australia's network performance (e.g. large email attachments can decrease system performance and potentially cause system outages).
- Does not incur any additional expense for Girl Guides South Australia.
- Does not compromise any confidentiality requirements of GGSA.

iv. Email security

Email is often vulnerable to hacker attacks, confidentiality breaches, viruses, and other malware. These issues can compromise our reputation, legality, and security of our organisation.

Staff and volunteers must:

- Select strong passwords with at least eight characters (capital and lower-case letters, symbols, and numbers) without using personal information (e.g., birthdays.)

- Remember passwords instead of writing them down.
- Keep passwords secret unless it is for the purposes of a shared email address (i.e. by leaders in a unit or those in shared roles) in which case a password is only to be shared between those persons for whom it is necessary to have access.
- Shared email address account holders should change the password following a volunteer with access to the account resigning from or leaving their position, negating the use of email access.
- As Guiding business is done through a range of GGSA addresses, it is imperative that those who require access to a shared account have the password made available to them (i.e. all unit leaders should have access to their unit's email account).
- Manually change their email password every two months, if this is not an automated process.

Staff and volunteers should always be vigilant to catch emails that carry malware or phishing attempts. We instruct them to:

- Only open emails when you recognise the sender and the email address.
- Avoid opening attachments and clicking on links when content is not adequately explained (e.g. "Watch this video, it's amazing.")
- Be suspicious of clickbait titles.
- Look for inconsistencies or style red flags (e.g., grammar mistakes, capital letters, excessive number of exclamation marks).

If an email account holder is not sure if an email, they have received is safe, they can refer to the Good Email Practice Guidelines for some help identifying spam or phishing email. Refer to GGSA Resources on SharePoint for access to these guidelines, alternatively contact Guide House who will assist.

Alternatively, email privacy@girlguidessa.org.au for advice. Issues will be resolved as quickly as possible; however, it should be noted that out-of-hours support may be limited.

Should you believe you have received any suspicious emails or believe you may have opened a suspect email or attachment – please email privacy@girlguidessa.org.au asap.

If staff or members have any other issues with accessing an authorised GGSA email account, please contact privacy@girlguidessa.org.au for assistance.

We remind our staff and volunteers to keep their virus protection and anti-malware programs updated on all devices and computers which they use to undertake Guiding business.

Staff and volunteers must not redirect corporate email accounts to personal accounts, regardless of whether these personal accounts have been set up only for Guiding purposes. Redirecting to and from personal accounts mean that security of data cannot be maintained.

v. Email signature

Guide House will be responsible for supplying volunteers and staff with a corporate email signature to be used in conjunction with Microsoft 365 account. Instructions will be provided to assist with setting up.

Updates will be supplied when required from Guide House.

vi. Representing Girl Guides South Australia

When staff and volunteers use company email, they act as representatives of GGSA at all times. If staff and volunteers use inappropriate language, it reflects negatively on GGSA and could create unnecessary reputational risk

Also, if a staff member or volunteer makes statements or promises using company email, the recipient may consider that anything the staff member or volunteer says represents the company's views, and that anything promised is binding.

Corporate emails are to be used for the following matters:

Any requests, conversations, raising of issues relating to the running, administration or leadership of the Unit, District, Region, Olave Peer Group, events, or a State Department.

Personal emails are to be used for the following:

- Enquiries about a member's own membership details.
- Matters confidential to individual members (complaints, performance, requests for leaves of absence etc.).

vii. Responses to emails from GGSA staff and volunteers.

Consider that staff and volunteers often conduct GGSA business on different days of the week and at different times of the day. This will affect how soon you may receive a response.

If you are emailing a staff member, please bear in mind their hours and days of working when expecting a response. If you are emailing a volunteer, please bear in mind that they are likely to be responding during evenings and weekends. In all cases, a follow-up phone call may assist if you are not receiving a timely response to your email.

4. Monitoring

GGSA accepts that the use of email is a valuable business tool. However, misuse of this facility can have a negative impact upon productivity and the reputation of the business.

The company's email resources are provided for business purposes. The company maintains the right to examine any systems and inspect any data recorded in those systems.

To ensure compliance with this policy, the company also reserves the right to use monitoring software to check upon the use and content of emails. Such monitoring is for legitimate purposes only.

GGSA has the right to monitor and archive corporate emails.

Individual email accounts are only to be accessed by those individuals (or multiple account holders if relevant) who hold them, unless:

- Access is requested by law enforcement in the investigation of a criminal offence; or
- In circumstances where the Board; or CEO of GGSA, the Chair of the GGSA Board and the GGSA State Commissioner each hold a reasonable suspicion that this, or a breach of other policies places the Organisation in serious risk, or that the health and/or safety of any person is at risk, they may access any email account they deem necessary.

5. Disciplinary action

Staff and volunteers who do not adhere to the present policy will face disciplinary action up to and including termination of employment and/or membership.

Reasons for termination may include:

- Using a corporate email address to send or intentionally receive confidential data without authorisation.
- Sending or intentionally receiving offensive or inappropriate emails to our customers, colleagues, or partners.
- Using a corporate email for an illegal activity.
- Using a corporate email non-Guiding business unless as permitted by this policy.
- Using a corporate email to distribute, disseminate, or store images, text or materials that might be considered indecent, pornographic, obscene, or illegal.
- Introducing any form of computer virus or malware into the corporate network.
- Accessing an email account without the necessary permissions or Authority.