SASTA ACCEPTABLE USE OF ELECTRONIC MEDIA POLICY

Introduction

The South Australian Science Teachers Association (SASTA) recognises that staff need access to email systems and the Internet to assist in the efficient and professional delivery of services. SASTA supports the right of staff to have access to reasonable personal use of the internet and email communications in the workplace.

Purpose

This policy sets out guidelines for acceptable use of the computer network, including internet and email, by employees and volunteers of SASTA. Access to internet and email is provided to SASTA staff and volunteers for the primary purpose of assisting them in carrying out the duties of their employment.

Policy

Staff may use the internet and email access provided by SASTA for:

- Any work and work-related purposes;
- Limited personal use (for details see Procedures, below);
- More extended personal use under specific circumstances (for details see Procedures, below).

Where staff use computer equipment or computer software at the premises of SASTA, or use SASTA equipment while working remotely (including from home), properly authorised staff of SASTA may access any data on that equipment to ensure that the organisation's policies are being adhered to. Such data should not be regarded as under all circumstances private in nature.

ACCEPTABLE USE OF ELECTRONIC MEDIA PROCEDURES

Definition

Electronic media includes all electronic devices and software provided or supported by SASTA, including, but not limited to, computers, electronic tablets, peripheral equipment such as printers, modems, fax machines, and copiers, computer software applications (including software that grants access to the internet or email) and telephones, including mobile phones, smartphones and voicemail systems.

Responsibilities

It is the responsibility of the EO to ensure that:

- staff are aware of this policy;
- any breaches of this policy coming to the attention of management are dealt with appropriately.

It is the responsibility of all employees and volunteers to ensure that their use of electronic media conforms to this policy.

Processes

Limited personal use

Limited personal use of computer, internet and email facilities provided by the organisation is permitted where it:

- Is infrequent and brief;
- Does not interfere with the duties of the employee or his/her colleagues;
- Does not interfere with the operation of SASTA;
- Does not compromise the security of SASTA or of its systems;
- Does not compromise the reputation or public image of SASTA;
- Does not impact on the electronic storage capacity of SASTA;
- Does not decrease network performance (e.g. large email attachments can decrease system performance and potentially cause system outages);
- Incurs no additional expense for SASTA;
- Violates no laws;
- Does not compromise any of the confidentiality requirements of SASTA;
- Does not fall under any of the "unacceptable use" clauses outlined below.

Examples of what would be considered reasonable personal use are:

- Conducting a brief online banking transaction, or paying a bill;
- Sending a brief personal email, similar to making a brief personal phone call.

Permitted extended personal use

It is recognised that there may be times when staff need to use the internet or email for extended personal use. An example of this could be when a staff member needs to use the internet to access a considerable amount of material related to study, they are undertaking.

In these situations, it is expected that:

- The staff member advise and negotiate this use with their manager beforehand in order to obtain the manager's approval;
- The time spent on the internet replaces all or part of a staff member's break/s for that day, or that they adjust their timesheet accordingly for that day.

Access to electronic data

SASTA may need to access any and all information, including computer files, email messages, text messages and voicemail messages. The organisation may, in its sole discretion, authorise its staff to inspect any files or messages recorded on its electronic media at any time for any reason. Where use of the organisation's equipment or software requires the use of a password, this should not be taken to imply any right of privacy in the user. The organisation may also recover information that a user has attempted to delete, and staff should not assume that such data will be treated as confidential.

Cyber Security

All staff and volunteers must take reasonable steps to protect SASTA's digital systems and information. This includes using strong, unique passwords and enabling two-factor authentication (2FA) where available. Any suspected data breaches, phishing attempts, or suspicious activity must be reported immediately to the Executive Officer.

Where personal devices are used to access SASTA systems or data, users must ensure these devices are secure, protected by a passcode or biometric lock, regularly updated, and not shared with others. All staff are strongly encouraged to complete basic cyber security awareness training, such as the *Cyber Wardens* course, to support safe digital practices.

Unacceptable use

Staff may not use internet or email access (including internal email access) provided by SASTA to:

- Create or exchange messages that are offensive, harassing, obscene or threatening;
- Visit websites containing objectionable (including pornographic) or criminal material;
- Exchange any confidential or sensitive information held by SASTA (unless in the authorised course of their duties);
- Create, store or exchange information in violation of copyright laws (including the uploading or downloading of commercial software, games, music or movies);
- Undertake internet-enabled activities such as gambling, gaming, conducting a business or conducting illegal activities;
- Create or exchange advertisements, solicitations, chain letters or other unsolicited or bulk email.

Authorisation

Dina Matheson
SASTA President

17 June 2025

Tegan McClean
Acting Executive Officer

17 June 2025

This policy is due for review in June 2028.