The Association of Graduates in Early Childhood Studies would like to acknowledge both the Bunurong/Boon Wurrung, and Wurundjeri people as the Traditional Custodians of the Lands on which we are located in Melbourne. We pay our respects to their Elders past, present and emerging. We also acknowledge the Aboriginal language groups across all of Victoria, whose lands we provide funding for specific projects around Early Childhood Education. We acknowledge their history, their people, and their stories. As an Association we will work together for reconciliation, a process that starts with the acknowledgement of true Aboriginal and Torres Strait Islander histories and cultures of Australia, and will always value the contribution to our community and culture, the experiences of Aboriginal and Torres Strait Islander peoples, their families, communities and their stories.

Cyber Security Policy and Procedure

Introduction

An effective cyber security policy is a responsibility of all Australian organisations. As AGECS operates entirely online, with software and data accessed by multiple people using their own computers, phone and devices, its key data is vulnerable to cyber-attacks.

Purpose

The purpose of this policy is to help Council members, AGECS committee members, contractors, consultants and ambassadors of AGECS to effectively identify, disclose and manage any actual, potential or perceived cyber risks in order to protect the integrity of AGECS and to manage its liabilities.

This policy sets out guidelines for generating, implementing and maintaining practices that protect the organisation's cyber media – computer equipment, software, operating systems, storage media, electronic data, and network accounts – from exploitation or misuse.

Scope

This policy applies to the Council members of AGECS and contractors.

Context

AGECS is a small organisation with simple IT systems relying on the security of 3rd party providers, volunteer Council and committee members, and contractors.

Policy

This policy has been developed to address cyber security risks affecting AGECS.

It is the policy of AGECS, as well as the responsibility of AGECS Council members and contractors, that good cyber security practices are upheld.

Council members, committee members and contractors will take all necessary measures to maintain the necessary cyber security procedures, including protecting passwords, securing access to computers, and maintaining protective software.

Compliance with this policy and procedure

Any major breaches of this policy would result in the activation of the AGECS complaints handling policy.

Review and storage of Cyber policy and procedure

This policy will be reviewed annually, saved on the AGECS shared documents platform and will guide periodic training. A hard copy must be available in the AGECS Manual in the event it cannot be accessed online during a cybersecurity incident.

For questions about this policy, contact the President.

Version	1	Approved by Council on	29/07/2024
Responsible person	The President	Scheduled review date	2027

Procedure

1. IT Contractor

AGECS I.T. environment is set up and managed by Consortium Pty Ltd (Unit 18 A/354 Reserve Rd, Cheltenham VIC 3192, tel: 1300 262 666) who have their own cyber security policies in place.

2. Responsibilities

It is the responsibility of the Program Manager to ensure that:

- Council members and contractors are aware of this policy;
- any breaches of this policy coming to the attention of AGECS are dealt with appropriately;
- Council is kept aware of any changes to the organisation's cyber security requirements;
- a report on the organisation's cyber security is submitted annually to Council.

It is the responsibility of all council members and contractors to ensure that:

- they familiarise themselves with cyber security policy and procedure;
- their usage of cyber media conforms to this policy and procedure.

3. Confidentiality

The Program Manager shall classify information in the AGECS's computer system files and databases as either non-confidential (open to public access) or confidential (in one or many categories and determine the appropriate level of security that will best protect it.

4. System Taxonomy

Security level	Description	Example
Red	This system contains confidential information – information that cannot be revealed to personnel outside AGECS. Even within AGECS, access to this information is provided on a "need to know" basis. The system provides mission-critical services vital to the operation of the business. Failure of this system may have an adverse impact on AGECS.	Server containing confidential data and other information on databases.
Green	This system does not contain confidential information or perform critical services, but it provides the ability to access RED systems through the network.	Individual user PCs used to access server and application(s).

Black	This system is externally accessible. It is isolated from RED and GREEN systems by a firewall. While it performs important services, it does not contain confidential information.	A public web server with non-sensitive information.

5. Data Taxonomy

Security level	Description	Example
Red	Client data allowing financial exploitation or identity theft Organisation data allowing banking or financial exploitation	Client credit card and banking data Organisational credit card and banking data Client details that would facilitate phishing
Green	Client data allowing address or email exploitation Organisational intellectual property that has financial or reputational consequences	Addresses that would facilitate spamming Internal emails
Black	Publicly accessible data	Non-sensitive information

6. Access control

The Program Manager will assign individuals clearance to particular levels of access to the organisation's information resources. Access control shall be exercised through username and password controls. Individuals shall access only those resources that they have clearance for.

Log-on IDs and passwords will be deactivated as soon as possible if the user leaves the organisation. The Program Manager shall directly contact the IT provider to report change in status that require terminating log-on access privileges.

7. User responsibility

As all AGECS assets are accessed by volunteers and contractors, AGECS has no control over those assets.

AGECS will manage this risk by annually requiring Council members and contractors to sign a Cyber Security acknowledgement, as below, as part of the Council Consent to Act form, and contractor annual contract.

Cyber Security

It is my responsibility to exercise due diligence in the use of personal devices for AGECS activities to ensure protection of AGECS data and resources.

I confirm I have undertaken the following actions on devices and software used for AGECS activities (including computer, tablets and mobile phone) – please tick:

- ☐ created and maintain strong passwords
- ☐ installed antivirus software
- ☐ installed automatic updates for software
- ☐ It is my responsibility to be careful when clicking on hyperlinks or opening attachments.
- ☐ I will contact the Program Manager as soon as I am aware my device/s may be compromised.

8. Threats

Phishing – Email phishing is one of the most common ways that hackers attempt to gain access to a network. The malicious email contains a link to an unknown source, which can unintentionally download malware on to the computer, giving hackers a window to the organisation's systems.

Social engineering fraud – It is a confidence scheme that intentionally misleads a person into sending money or diverting a payment based on fraudulent information that is provided to the person in a written or verbal communication such as an email, letter or a phone call.

Unusual password activity – If you're locked out of your system or you receive an email stating that a password has been changed, it is a potential sign that the password has been compromised, or that someone is attempting to log into your account.

Slower than normal network – A hacking attempt or malware infection often results in spikes in network traffic that can reduce internet speed.

Identify suspicious pop-ups – you should avoid clicking on pop-ups while browsing the internet. Unknown pop-ups can be infected with malware or spyware, which can compromise your computer/devices.

9. Prevention

- Human error is a major cause of cyber security incidents.
- Devices should be locked when unattended and any theft or loss of devices containing AGECS data should be reported to the Program Manager.
- All PCs, laptops and devices should be secured by a password-protected screensaver with the automatic activation feature set at 10 minutes or less, or by logging-off when the device will be unattended. A passphrase (consisting of at least 14 characters and usually a combination of unrelated words) offers stronger protection than a password and should be utilised whenever possible. It is acceptable to use password managers from reputable vendors using industry standard encryption to store the password. Further information about passphrases:

https://www.cyber.gov.au/protect-yourself/securing-your-accounts/passphrases/creating-strong-passphrases

- Users should keep passwords secure. Accounts must not be shared, and no other people may be permitted to use the account. Passwords should not be readily accessible in the area of the computer concerned. Authorised users are responsible for the security of their passwords and accounts.
- All computers and devices used by the user that are connected to the AGECS programs including OneDrive should be continually executing virus-scanning software.
- Malware protection software should not be disabled or bypassed, nor the settings adjusted to reduce their effectiveness.
- Automatic daily updating of the malware protection software and its data files should be enabled.
- All email attachments should be scanned. Weekly scanning of all computers should be enabled.
- Users should periodically review email security settings – instructions to do this are available here: https://www.cyber.gov.au/report-and-recover/recover-from/email-compromise/what-do-if-youve-been-attacked/review-your-email-account-security
- Data on laptops and devices should be protected by full disk encryption.
- Microsoft Edge, Google Chrome or Safari are recommended web browsers with all auto updates enabled when accessing AGECS programs on private devices.
- When on AGECS business, users should not use public wi-fi access.
- Home wi-fi networks should be encrypted using a WPA2 router or greater and use a strong and memorable password that is changed periodically.
- Users must use extreme caution when opening email attachments received from unknown senders; these may contain viruses, malware or Trojan horse code.
- Users who believe their devices and systems have been subjected to a security incident, or has otherwise been improperly accessed or used, should report the situation to the Program Manager immediately.

Appropriate caution will be exercised when:

- sharing any email address utilised to access AGECS information
- opening email attachments, ensuring they are only from trusted sources/contacts

Users should:

- block junk, spam and scam emails
- identify and delete suspicious looking emails, text messages, phone calls and social media messages. Such correspondence is characterised by presence of file extensions within attachments, suspicious links, unusual email senders, poor spelling and a sense of urgency.

10. Handling of sensitive data

- AGECS holds personal information including member contact details
- These details are held in the WordPress database and Mailchimp protected by 2FA, and an Excel spreadsheet which is password protected.
- Data including names and addresses will not be distributed beyond approved personnel

- Data should be regularly backed-up to prevent data loss and restoration of data should be tested periodically by the Program Manager

11. Cyber-incident response

In the event of a cyber incident, AGECS will be guided by the Australian Government's Office of the Australian Information Commissioner recommendations:
https://www.oaic.gov.au/privacy/privacy-guidance-for-organisations-and-government-agencies/preventing-preparing-for-and-responding-to-data-breaches/data-breach-preparation-and-response/part-3-responding-to-data-breaches-four-key-steps

Suspicious activity indicating a cyber-incident may include:

- Accounts no longer accessible
- Passwords/passphrases not operating
- Missing, altered data or inaccessible files
- Hard drive runs out of space unexpectedly
- Computer keeps crashing
- SPAM is received from an official AGECS email account
- Numerous pop-up ads and error messages
- Unauthorised debits from bank accounts

All suspicious activity relating to AGECS is to be reported to the Program Manager as soon as practical. Early detection of a cybersecurity incident is critical.

12. Cyber insurance

AGECS will take out annual cyber insurance.

Such insurance asks the following:

- Do you run commercially licensed firewalls and antivirus?
- Do you enforce a policy of auditing and managing computer and user accounts?
- Are all mobile devices (such as laptops, tablets, smartphones and memory sticks) password protected?
- Are you Payment Card Industry (PCI) compliant, if applicable? If not applicable, leave blank
- Does the Disaster Recovery Plan or Business Continuity Plan take Cyber and data risks into consideration?
- Network Dependency - after how long will your business be impacted by a loss to your site/systems?
- Have you ever been investigated in respect of personally identifiable information, including but not limited to payment card information, or your privacy practices?
- Have you been asked to supply any regulator or similar body with information relating to personally identifiable information or your privacy practices?
- Have you ever received a complaint relating to the handling of someone's personally identifiable information?
- Do you back up critical data at least once a week?
- Do you outsource any critical systems/applications to third parties?

13. Cyber security 3rd parties

Organisation	Link to Security Info	MFA Enabled
ANZ		
EVANS & PARTNERS		
EVENTBRITE		
MAILCHIMP	https://mailchimp.com/legal/	
MICROSOFT 365	https://www.microsoft.com/en-au/trust-center/privacy	
PAYPAL	https://www.paypal.com/us/legalhub/privacy-full	
WESTPAC	https://www.westpac.com.au/content/dam/public/wbc/documents/pdf/privacy/Westpac_Privacy_Statement.pdf Not much about security	
XERO	https://www.xero.com/content/dam/xero/pdfs/legal/xero-privacy-notice-july-2020.pdf	
ZOOM		

14. Useful contacts

The Australian Cyber Security Centre
1300 292 371 (24 hrs / 7 days a week)

Office of the Victorian Information Commissioner
https://ovic.vic.gov.au/

15. Sample notice to affected individuals

Template from the Office of the Victorian Information Commissioner:
https://ovic.vic.gov.au/privacy/resources-for-organisations/privacy-officer-toolkit/data-breaches/

[Affected individual's name]
[Affected individual's address]
[Date]

Notification of privacy incident

Dear [affected individual's name],
We are writing to let you know about a recent privacy breach that involved some of your personal information. This letter will explain what happened, how we have responded and what it means for you.

What happened?
[On/between] [date/time period], [provide a summary of the incident, why it constitutes a breach and steps you have taken to investigate what happened]

This section should be detailed so the person has a good understanding of what occurred and why what occurred is considered a privacy breach. The language should be clear and tailored such that a layperson with no technical experience can understand the nature of the breach. It is often helpful to use the active rather than passive voice. You should also be as specific as possible e.g. instead of referring to a 'third party' you may wish to identify the third party or at least describe the type of third party.

What information was affected?
Based on our investigation, we understand that your personal information that has been affected by this incident includes:
· [List the personal information affected].
Examples of personal information include: name, residential address, phone number, credit card number or the fact the individual made a complaint to the organisation.

Details about the personal information involved will allow affected individuals to make their own assessment about the likely harm that they may experience because of the incident and develop proactive steps to protect themselves.

What have we done in response to the breach?
[Describe the steps you have taken or are intending to take to contain the breach and minimise any potential harm.]
[Describe the steps you have taken or are intending to take to reduce the likelihood of similar incidents occurring in the future.]

This information may help an affected individual feel reassured about your organisation's response and information handling practices; reduce any distress they initially experienced; and impact their own risk assessment.

What does this mean for you?
You should carefully review the information that was affected by this incident and think about whether this could result in you experiencing any harm. Some of the steps you may consider taking to protect yourself include:
[Example - Where the risk of harm is identity fraud]
· Be aware of emails and telephone calls from people requesting your personal details, (especially things like your date of birth, residential address, email address, username or passwords which are often used to verify your identity).

- Change your account password.
- Contact IDCare on 1300 432 273 or visit www.idcare.org who can provide you with
- additional guidance on the steps you can take to protect yourself from identity
- fraud. [Example - Where the risk of harm is spam]
- If you start to receive unwanted telemarketing calls, consider registering your

- number with the Australian Communications and Media Authority's 'Do Not Call
- register' by visiting www.donotcall.gov.au/consumers/register-your-numbers . You
- can also contact your service provider and request to change your number.
- [Example - Where the risk of harm involves financial information]
- Alert your financial institution so that they can implement additional monitoring and
- security protocols on your account.
- Closely monitor your financial statements for unauthorised transactions. If you
- identify a transaction you didn't make, report it immediately to your financial
- institution.
- Change your online bank account password, banking PIN and enable multi-factor
- authentication if possible.
- Contact Australia's three credit reporting agencies (Equifax, illion and Experian) to
- confirm if your identity has been used to obtain credit without your knowledge or to
- request for a credit ban to be put in place.
- [Where the information affected includes TFN or superannuation details]
- Contact the Australian Tax Office on 1800 467 033 or your superannuation fund so
- that they can consider placing additional monitoring and security protocols on your
- account.

Further information is also available on the Office of the Victorian Information Commissioner's website at www.ovic.vic.gov.au/privacy/for-the-public/data-breaches-and-you .

More information and making a complaint

If you have any concerns about what has happened or would like further information, you can contact:
[individual or department's name within your organisation]
[phone number] or [email].

If you are not satisfied with how we have handled this incident or you have experienced some harm as a result, you can make a privacy complaint. You can do so by contacting us by email at [email]. It would be helpful if you could explain how you have been affected by the breach and what you would like us to do to resolve your complaint.

If we cannot resolve your complaint, you can then make a complaint to the Office of the Victorian Information Commissioner (OVIC). You can find out more about how to make a complaint to OVIC at https://ovic.vic.gov.au/privacy/for-the-public/complaints/ .

Yours sincerely,

[Name of representative]
[Position of representative]
[Organisation