POLICY No. 26 Cybersecurity Policy

Applies to:	**Board, Staff, Club Committee Volunteers, Teachers and Inpool volunteers**
Responsibility:	**IT Manager**
Status	**Approved Dec 2022**
	Date for review 11/2023

Policy Statement

Rainbow Club protects its electronic information from unauthorised access and this policy and the procedures that follow apply to all electronic information gathered and stored by Rainbow Club Australia.

It is Rainbow Club's policy to ensure that all staff and volunteers have a basic understanding of cyber security issues.

This policy and procedures should be read in conjunction with Policy 106 – Collecting, storing and disposing of information.

Policy 106 Privacy - Collecting, storing and disposing of Information
Rainbow Club only collects and stores personal information that is necessary for the function of the organisation and its activities. All records are stored on the Rainbow Club digital platforms and disposed of after the legal requirements to keep records has expired

Policy 106 - Access to Information
Rainbow Club will prevent unauthorised persons gaining access to an individual's confidential records and permit individuals' access to their own records when this is reasonable and appropriate.

Rainbow Club recognises that common cybersecurity risks include:

- unauthorised access to a device, network or system
- viruses or other malicious software that can collect, change or delete information and spread throughout a network
- fake emails or websites set up to trick someone into revealing personal or sensitive information.

Rainbow Club acknowledges that the consequences of any incident can be significant and may include:

- loss of crucial information
- disruption to services
- unauthorised changes to Rainbow Club's information and systems
- expensive costs to restore data and services

- costs of notification and investigation (including legal costs)
- costs arising from the attack itself (for example, extortion or ransomware)
- regulatory action and penalties
- loss of trust and reputation

Protecting Rainbow Club from cyberattacks

Everybody at Rainbow Club has an important part to play in protecting against cyberattacks, the ultimate responsibility is with the General Manager, Shared Services Manager and IT Manager

It is their role to make sure that they have plans to

- Identify and assess the risks
- Prevent incidents and mitigate risks
- Engage people in Rainbow Club and its providers to help manage risks
- Take action when concerns, suspicion or complaints arise.

Lifecyle of Data Breach	
Data held by Rainbow Club	**System, Data and Storage Methods**
Identify Risks	
Consider what types of data your organisation holds, and how you store that data	**Salesforce Member information:** Member Contact details, age, gender, disability, goals, progress in learning to swim **Salesforce Teacher information:** Teacher Contact details, age, gender, qualifications, Pay Level, Covid Vaccine info **First Class Member information:** Member Contact details, age, gender disability, goals, progress in learning to swm and payment transaction details **Sharepoint** Organisation files **Website Data** Website content – text, photos **Payroll Information** All payroll data is stored on ADP Payroll Solutions systems
Protect your systems	
Firewalls and Anti-malware software	We do not have a firewall as we are running off Office365. Office 365 has the benefit of built-in, high-end security. Rainbow Club ensures that all company laptops have the appropriate antivirus/malware software.

Use 2 factor authentication, regularly update passwords and ensure complexity requirements for passwords are high	MFA is enabled for our Salesforce CRM system and ADP.
Provide regular staff member training on cyber risks	Staff awareness on cybersecurity will be made prior to end of 2022 and then ongoing in 2023
Respond to threats	
Create a simple, easy to follow data breach response plan	– See following
Recover from impacts	
Save regular backups of your key servers so previous versions can be restored if there is a data breach	See Compliance Report

In the event of a Data Breach, Rainbow Club has the following plan to follow

Data Breach Incident Plan

A data breach is when protected information is accessed or disclosed without authorisation. The people responsible for each action of the plan will be in charge of making sure the plan is followed.

Mandatory training/awareness for all staff will be delivered regularly.

Step	Action	Person responsible
1. Identify	Report the actual or suspected data breach immediately to **IT Manager**.	
	Decide whether an actual or suspected data breach has occurred. [Use the OAIC guide to identify if an eligible data breach has occurred or not].	IT Manager
	The individual who discovered the breach should take note of the following details, and pass the information to the co-ordinator: • The time and date of the actual or suspected data breach • The type of information involved • Ways the data breach can be contained	
2. Investigate	Investigate the breach and assess: • The information involved in the data breach • The cause of the breach • The extent of the breach • People who have been, or may be, affected • The extent of the harm • The need to notify the people affected, and what information they need to know.	IT Manager Shared Services Manager General Manager
3. Assess	Assess each threat identified from the breach based on the information gathered during the investigation. This assessment should consider whether: • There has been any loss, misuse or disclosure of information • There is a risk of harm to individuals because of the breach (for example, has it revealed personal or sensitive information?) • Actions have been taken to reduce the risk of harm • There is a need to notify affected people or relevant regulators	IT Manager Shared Services Manager General Manager Programs and Quality Manager
	Record the details of the assessment and keep it filed (physically or electronically). Make sure people who need to see it get a copy or can access it easily.	IT Manager
4. Notify	Notify the affected people, organisations and regulators. Consider whether: • The notification needs to happen within 12 hours • The notification needs to be in a particular format (for example, an email or a letter) • Rainbow Club will publish a public notification on its website or social media pages **Reporting Critical Cyber Security Incidents** If Rainbow Club Australia becomes aware that a **critical cyber security incident** has occurred, or is occurring, AND the	IT Manager

Step	Action	Person responsible
	incident has had, or is having, a **significant impact on the availability of our system,** the Australian Cyber Security Centre (ACSC) will be notified **within 12 hours** after becoming aware of the incident. A significant impact is one where both the critical systems used in connection with the provision of essential goods and services; and the incident has materially disrupted the availability of those essential goods or services.	
5. Review	Review the data breach and the response. Record the findings and make a list of recommendations for improvements. Make sure the review covers the following: • An understanding of how the breach occurred • Updates to processes for managing information and data to prevent another breach occurring • Updates to other relevant policies and procedures to reflect changes • Employee training for dealing with the private and confidential information	IT Manager Shared Services Manager General Manager Programs and Quality Manager