INFORMATION TECHNOLOGY POLICY

2026 / 2027

Version 3.0

March 2026

1. PURPOSE

The purpose of this Information Technology Policy is to:

- Protect the confidentiality, integrity and availability of the organisation's information systems.
- Ensure all technology resources are used responsibly, ethically and legally.
- Protect broadcast operations from accidental or deliberate disruption.
- Reduce the risk of malware, ransomware, cyber-attacks and data breaches.
- Provide clear rules regarding the use of computers, networks, removable media, email systems and internet services.
- Ensure compliance with applicable legislation, broadcasting requirements and privacy obligations.

This policy applies to all employees, volunteers, contractors, board members, presenters, producers, trainees and any other persons granted access to the organisation's technology systems.

2. SCOPE

This policy applies to:

- Desktop computers
- Laptops
- Studio computers
- Broadcast automation systems
- Audio production systems
- Streaming systems
- Mobile devices
- Servers
- Cloud services
- Email systems
- Network infrastructure
- Internet services
- Storage devices
- All organisation-owned and personally-owned devices connected to organisation systems

3. ACCEPTABLE USE

Users must:

- Use systems only for authorised station activities.
- Protect organisation information.
- Follow all security requirements.
- Report security incidents immediately.
- Respect copyright laws and software licensing requirements.
- Use technology resources professionally and responsibly.

Users must not:

- Access systems without authorisation.
- Share passwords.
- Install unauthorised software.
- Circumvent security controls.
- Use systems for illegal activities.
- Access offensive, discriminatory or inappropriate material.
- Download copyrighted material without permission.
- Use organisation resources for personal commercial activities without written consent.

4. USER ACCOUNTS AND ACCESS

4.1 Individual Accounts

Each authorised user shall be provided with their own account where practical.

Shared accounts should only be used where operationally necessary, such as:

- Broadcast automation systems
- Studio playback systems
- Public information terminals

4.2 Access Levels

Access shall be granted on the principle of least privilege.

Members shall only receive access required to perform their duties.

Access levels may include:

- Volunteer
- Presenter
- Producer
- Department Manager
- Technical Team
- Administration
- Executive Management
- Board Member

4.3 Account Suspension

Access may be restricted, suspended or withheld for any reason if:

- The member has been stood down pending a formal investigation; and or
- The member has been suspended due to breaches of policies & procedures; and or
- The member has left the organisation; and or
- The member has abandoned their duties; and or
- The member has taken a leave of absence approved by the board of directors

4.4 Account Removal

Access shall be removed immediately when:

- A volunteer leaves the organisation.
- Employment ceases.
- Access is no longer required.
- A security risk is identified

5. PASSWORD REQUIREMENTS

Passwords must:

- Be at least 12 characters long.
- Contain a mixture of letters, numbers and symbols.
- Not be easily guessed.
- Not contain personal information.

Users must not:

- Share passwords.
- Allow their password or access to be used by any other person without the written authority of the board and the Information Technology Officer
- Write passwords on equipment.
- Store passwords in unsecured documents.

By default, multi-factor authentication is enabled and used throughout the organisation where possible.

6. COMPANY EMAIL SYSTEMS

6.1 Official Communications

Organisation email accounts shall be used for:

- Station business.
- Sponsor communications.
- Volunteer communications.
- Community engagement.
- Regulatory matters.
- Financial and administrative activities.

6.2 Email Ownership

All email accounts provided by the organisation remain the property of the organisation.
Users should have no expectation of privacy regarding organisational records.

6.3 Prohibited Email Activities

Members must not:

- Send offensive messages.
- Send discriminatory material.
- Send chain letters.
- Send spam.
- Send confidential information without authorisation.
- Use organisation email for unlawful purposes.
- Use any other email service (such as Gmail, Hotmail, Yahoo, Outlook.com etc) for organisation purposes

6.4 Phishing Awareness

Users must:

- Verify suspicious emails.
- Report suspected phishing attempts.
- Not open suspicious attachments.
- Not provide passwords via email.

If in doubt over the origin of an email or its attachment. Please see the Information Technology Officer

7. REMOVABLE MEDIA POLICY

7.1 General Requirements

Removable media includes:

- USB drives
- USB hard drives
- CDs
- DVDs
- SD cards
- Mobile phones used as storage devices

All removable media represents a significant security risk.

7.2 Bringing Media Into the Station

No removable media may be connected to organisation systems unless:

- It is owned by the organisation; or
- It has been approved by the Information Technical Officer Department.

Users bringing content into the station must:

- Present media for scanning.
- Ensure content is legally obtained.
- Ensure content is free of malware.

7.3 USB Devices

The following rules apply:

- Unknown USB devices must never be connected.
- Found USB devices must never be connected.
- Personal USB devices require approval.
- All USB devices must be virus scanned.

The organisation reserves the right to disable USB access on all broadcast systems. This includes studios and production machines

7.4 Audio CDs

Presenters and volunteers may bring audio CDs into the station provided:

- The material is legally owned.
- Content complies with station policies.
- The CD is scanned where possible before importing.
- Only authorised staff may permanently import music into station systems.

7.5 External Hard Drives

External drives must:

- Be approved by Technical Management.
- Be scanned before use.
- Be used only for approved operational purposes.

8. SOFTWARE INSTALLATION

Users must not install software without approval.

This includes:

- Audio editing software
- Browser extensions
- Utilities
- Streaming software
- Mobile applications
- Games

All software installations must be authorised by the Technical Team.

9. INTERNET USAGE

Internet access is provided for organisational purposes.

Limited personal use may be permitted provided it:

- Does not interfere with operations.
- Does not consume excessive bandwidth.
- Does not breach organisational policies.

Users must not:

- Breach our social media policy
- Access illegal content.
- Download pirated software.
- Access malicious websites.
- Engage in online harassment, bullying.
- Engage in any other illegal activities

10. SOCIAL MEDIA AND ONLINE SERVICES

Only authorised personnel may represent the organisation online (such as on facebook, twitter, snapchat etc).

Passwords for organisation social media accounts must:

- Be centrally managed.
- Be changed when personnel change.
- Not be shared outside authorised personnel.
- Must not be accessed or used on non-approved devices

Official accounts remain the property of the organisation.

11. BROADCAST SYSTEM SECURITY

Broadcast systems are considered critical infrastructure.

Users must not:

- Modify automation schedules without authority.
- Install software on studio computers.
- Alter streaming settings.
- Modify broadcast processors.
- Change network configurations.

Only authorised technical personnel may perform these functions.

12. DATA STORAGE

Organisation data shall be stored only on approved systems.

Users must not store organisational data solely on:

- Personal computers
- Personal cloud accounts
- Personal USB drives

Approved storage locations include:

- Organisation servers
- Approved cloud platforms
- Approved backup systems

13. BACKUP AND RECOVERY

The organisation shall maintain backups of critical systems.

Users must ensure important files are stored on approved systems to allow inclusion in backup processes.

14. COPYRIGHT COMPLIANCE

Users must comply with:

- Copyright legislation
- Music licensing agreements
- Broadcast licensing requirements
- Software licensing requirements
- Unauthorised copying or distribution of copyrighted material is prohibited.
- Removal of licenced software without written consent of the Technical Officer is prohibited.

15. PERSONAL DEVICES (BYOD)

Members who have dedicated office staff, may where permitted by the board of directors bring their own property into and store on the premises. This hardware is the sole property of the member

Personal devices may be connected only where approved.

The organisation may require:

- Antivirus protection
- Device encryption
- Password protection
- Security updates
- Access may be revoked at any time.

16. INCIDENT REPORTING

Users must immediately report:

- Lost devices
- Stolen devices
- Malware infections
- Suspicious emails
- Unauthorised access
- Data breaches
- Security weaknesses

Reports should be made to the Technical Manager or Station Manager.

17. MONITORING

The organisation reserves the right to monitor:

- Email usage
- Internet usage
- System access logs
- Network activity
- File transfers
- Security events

Monitoring is conducted to:

- Protect systems.
- Investigate incidents.
- Ensure compliance.

18. DISCIPLINARY ACTION

Failure to comply with this policy may result in:

- Verbal warning
- Written warning
- Suspension of system access
- Suspension of volunteer duties
- Termination of employment
- Cancellation of membership
- Referral to law enforcement where appropriate

Author:	Matthew Berry	**Reviewed By:**	Matthew Berry
Revised Date:	June 2026	**Next Revision Date:**	June 2027
Approved By	Board Of Directors	**Version:**	3.0