Policy Title:	Information Technology (IT) Policy
Policy Number:	17
Last Amended Date:	11/04/2025
Supersedes:	N/A
Author:	Operations Manager
Owner:	Chief Executive Officer
Endorser:	Lionheart Board
Date Endorsed:	18/08/2025
Next Review Due:	18/08/2026

INTRODUCTION

Lionheart Camp for Kids (Lionheart) is committed to ensuring the responsible, secure, and lawful use of information technology (IT) resources within the organisation. This policy establishes clear guidelines for the use, security, and management of IT systems, protecting sensitive data and ensuring compliance with Western Australian (WA) and Commonwealth (Cth) legislation and Australian Charities and Not-for-profits Commission (ACNC) governance standards.

PURPOSE

The purpose of this policy is to:

- Ensure the appropriate use of IT resources within Lionheart.
- Safeguard organisational and participant data.
- Protect IT systems from cyber threats and misuse.
- Comply with relevant privacy, security, and governance laws.
- Outline roles and responsibilities for IT management.

DEFINITIONS

- *IT Resources:* Includes computers, mobile devices, software, cloud services, email, internet, and network access.
- *Cybersecurity:* Measures taken to protect IT systems from unauthorised access, attacks, and data breaches.
- *Data Breach:* Unauthorised access, disclosure, or loss of personal or sensitive information.
- *Malware:* Harmful software designed to damage, disrupt, or gain unauthorised access to IT systems.
- *Multi-Factor Authentication (MFA):* A security process requiring two or more verification methods for access.

POLICY

1. Acceptable Use of Organisation Owned IT Resources

- IT resources must be used for legitimate work-related activities.

2. Data Security and Privacy

- All organisational and participant data must be securely stored and accessed only by authorised personnel using the organisation's credentials.
- Personal and sensitive data must be handled in compliance with the Privacy Act 1988 (Cth).
- Employees and volunteers must not share passwords or leave devices unsecured.

3. Cybersecurity Measures

- Anti-virus and anti-malware software must be installed and regularly updated.
- Multi-Factor Authentication (MFA) must be enabled where possible.
- Cyber security awareness training must be conducted annually.

4. Email and Communication

- Organisational email accounts must be used for work-related communications.
- Personal email accounts must not be used to transmit Lionheart-related information.
- All content must be written in clear, inclusive, and trauma-informed language, avoiding clinical and/or technical jargon. Accessibility standards—such as providing alternative texts, captions, and easy-read formats—must be upheld to ensure content is inclusive and accessible to everyone.
- The Spam Act 2003 (Cth) prohibits sending unsolicited emails.

5. Social Media and Online Conduct

- Employees and volunteers must not access, download, or distribute illegal and/or inappropriate content.
- Employees and volunteers must not share confidential or sensitive information on social media. Refer to *Our People Policy* for disciplinary action procedures.
- Images, audio, or video of children involved in Lionheart programs must not be posted online without prior written media consent from their legal guardians. Employees and volunteers must ensure content respects the dignity and privacy of bereaved children and families.
- When representing Lionheart online, individuals must act professionally and in line with the organisation's values. This includes, but is not limited

to, interactions such as:

  - Replying to comments on Lionheart’s social media posts
  - Replying to direct messages on Lionheart’s social media platforms

- Employees and volunteers are personally responsible for content they share on their social media accounts and need to ensure they avoid engaging in inappropriate behaviour, ensuring interactions are aligned with Lionheart’s values.

6. Remote Work and Bring Your Own Device (BYOD)

- Employees and volunteers using personal devices for work must ensure data security. Lionheart equipment should be prioritised for primary use whenever possible over BYOD.
- VPNs should be used when accessing organisational data remotely.

7. Incident Reporting and Data Breach Response

- Any suspected IT security incident must be reported immediately to the Operations Manager.
- Serious breaches (such as but not limited to incidents involving child data or multiple users) must be escalated to the CEO and Board Director (IT) within 4 hours for a coordinated response.
- Data breaches must be managed in accordance with the Notifiable Data Breaches (NDB) scheme under the Privacy Act 1988 (Cth).

8. Maintaining up-to-date information across Lionheart website and social media accounts

- Lionheart is committed to maintaining accurate, up-to-date, and relevant information on its website and social media platforms to ensure clear communication with stakeholders.
- All online content must align with Lionheart’s mission, branding guidelines, and privacy obligations.
- Website and social media updates should be reviewed regularly to ensure accuracy, accessibility, and compliance with applicable laws and best practices.

PROCEDURE

1. **User Access and Security**
   - New employees and volunteers must be provided with appropriate IT access upon onboarding by the Operations Manager or specified delegate.
   - Access rights must be reviewed regularly and revoked upon

termination.

2. **Data Backup and Recovery**
   - Organisational data must be backed up daily to prevent data loss.
   - Backups must be stored securely and tested periodically.
3. **IT Support and Maintenance**
   - IT systems must be regularly updated and maintained by Board Director (IT) or identified Operational delegate.
   - IT issues must be reported to designated support personnel as above.
4. **Reporting Security Incidents**
   - Any cybersecurity threat, suspected hacking attempt, or unauthorised access must be reported immediately.
   - A formal investigation will be conducted to assess the incident and implement corrective actions.
5. **Equipment and System Suitability**
   - Board Director IT (or Operational delegate) is accountable for identifying suitable physical IT equipment and IT systems for operational use. Operations Manager is accountable for the usage of such equipment to suit the organisation's business needs.
6. **Updating website and social media accounts**
   - Website Updates: Designated employees will review and update website content at least quarterly or as needed for major announcements.
   - Social Media Management: Posts must be planned, reviewed, and scheduled in accordance with Lionheart's marketing strategy, with timely responses to interactions where appropriate.
   - Social Media Content: Designated employees will meet regularly to review and plan future content.
   - Monitoring & Review: Online content will be periodically reviewed to remove outdated information, correct errors, and ensure consistency across platforms.

REVIEW

This policy will be reviewed annually or when significant IT security or legal changes occur to ensure continued effectiveness and compliance.

RELATED DOCUMENTS

- Record-Keeping Policy
- Confidentiality Agreement

- Our People Policy
- External Feedback Policy

REFERENCES

- Privacy Act 1988 (Cth)
- Notifiable Data Breaches (NDB) Scheme
- Spam Act 2003 (Cth)
- Copyright Act 1968 (Cth)
- ACNC Governance Standards
- WA State Government Cyber Security Policy

KEY CONTACT PERSON

For further information please contact the Operations Manager by emailing enquiries@lionheartcampforkids.com.au.