



Darwin Education Information Security Policy

Policy Owner: Natalie Wilsher, Director

Applies to: All staff, contractors, volunteers, and systems

1. Purpose

The purpose of this policy is to ensure the confidentiality, integrity, and availability of information and IT systems used by Darwin Education. This policy aims to protect organisational, staff, and learner information from unauthorised access, loss, disclosure, alteration, or destruction.

2. Scope

This policy applies to all devices, networks, systems, applications, and data owned, managed, or used by Darwin Education, including cloud-based services and personal devices authorised for work purposes.

3. Access Control

- All users must have a unique user account.

- Access to systems and information must be granted according to the principle of least privilege.
- User accounts must only be created following authorisation by management.
- Accounts must be disabled or removed promptly when no longer required, including when a staff member leaves the organisation.
- Administrative privileges must be restricted to authorised personnel only.
- User access rights will be reviewed periodically to ensure they remain appropriate.

4. Password Requirements

- Passwords must be strong, unique, and not shared with any other person.
- Passwords should be a minimum of 12 characters where the system allows.
- Default passwords supplied with devices or systems must be changed before use.
- Multi-factor authentication (MFA) must be enabled on all systems where available.

5. Device Security

- All devices must be protected by a password, PIN, or biometric authentication method.
- Devices must not be left unattended while logged in.
- Devices must be configured to lock automatically after a period of inactivity.
- Updates and security patches must be applied regularly.
- Lost or stolen devices must be reported immediately.

6. Malware Protection

- All organisational devices must have approved anti-malware protection installed and enabled.
- Real-time protection must remain active at all times.
- Security software must not be disabled without authorisation from IT.
- Malware detections and alerts must be investigated promptly.

7. Security Updates

- Security updates must be applied as soon as reasonably practical.
- Critical and high-risk vulnerabilities should be addressed within 14 days where possible.
- Unsupported operating systems and software must not be used on organisational devices.

8. Network Security

- Firewall protection must be implemented and maintained.
- Secure wireless networks must be used, and open or unsecured networks must not be used for organisational activities.
- Access to network infrastructure and administration systems must be restricted to authorised personnel.
- Network equipment must be configured securely and reviewed periodically.

9. Remote Access

- Remote access to organisational systems must be conducted through secure and approved methods.
- Remote access accounts must be protected by multi-factor authentication where available.
- Users accessing systems remotely must ensure they are working in a secure environment.

10. Incident Management

- Any suspected information security incident must be reported immediately to the IT Lead or management.
- Security incidents, including suspected malware infections, unauthorised access attempts, lost devices, and data breaches, must be investigated promptly.
- Incidents will be documented and reviewed to identify lessons learned and opportunities for improvement.

11. Acceptable Use

- Users must comply with all organisational policies relating to the use of information technology.
- Organisational systems and devices must only be used for authorised purposes.
- Users must take reasonable steps to protect organisational information and equipment.

12. Responsibilities

Management

- Ensure appropriate resources are available to implement this policy.

- Review information security risks and incidents.

IT Lead

- Implement and maintain technical security controls.
- Monitor compliance with this policy.
- Investigate and respond to security incidents.

All Users

- Follow the requirements of this policy.
- Protect organisational information and equipment.
- Report security concerns or incidents immediately.

13. Policy Review

This policy will be reviewed annually or sooner if significant changes occur to systems, legislation, or organisational requirements.

Policy Details

Written by: Natalie Wilsher, Director

Owner: Natalie Wilsher, Director

Date Approved: September 2026

Next Review: September 2027