



IT, Systems & Acceptable Use (including Social Media) Policy

Policy Owner: Director

Applies to: Workers, including employees, casual employees, interpreters, volunteers, contractors, consultants, and representatives acting on behalf of Echo Interpreting.

Effective Date: 2 June 2026

Review Cycle: Every 2 years or as legislation changes or operational requirements change.

1. Purpose

Echo Interpreting relies on information technology, digital systems, and online platforms to deliver professional interpreting services.

This policy sets clear expectations for the appropriate, responsible, and secure use of IT systems, devices, and social media when undertaking work for Echo Interpreting.

This policy recognises the high-trust nature of interpreting work, particularly where workers may access sensitive personal, health, disability, legal, workplace, and confidential information.

2. Scope

This policy applies to all workers and representatives of Echo Interpreting, including:

- Employees
- Casual employees
- Interpreters
- Volunteers
- Contractors and consultants, where applicable
- Management and representatives acting on behalf of Echo Interpreting

It applies to:

- All Echo Interpreting IT systems and platforms
- Microsoft 365 / SharePoint / Teams (where applicable)
- Personal devices used for work purposes
- Remote, mobile, and client-site work
- Work-related events, meetings, and activities
- Online and social media activity connected to Echo Interpreting

3. Legislative Framework

This policy is informed by and aligned with relevant Australian and Victorian legislation, including but not limited to:

- Privacy Act 1988 (Cth)
- Australian Privacy Principles (APPs)
- Notifiable Data Breaches Scheme (Cth)
- Health Records Act 2001 (Vic), where applicable
- NDIS Code of Conduct Rules 2018

4. Systems and Technology Covered

This policy applies to all systems and tools used for Echo Interpreting work, including but not limited to:

- Email and calendars
- Booking and scheduling systems
- File storage and cloud platforms
- Messaging services (SMS, WhatsApp, Teams, etc.)
- Video Remote Interpreting (VRI) platforms and online interpreting systems
- Business websites and social media accounts
- Personal devices used for work purposes
- Artificial intelligence (AI) tools and other digital productivity platforms used for work purposes

5. Acceptable Use Principles

All users must:

- Access only information required for their role or assigned work
- Use systems primarily for legitimate business purposes
- Act professionally, ethically, and responsibly at all times
- Protect confidential and personal information
- Follow Echo Interpreting policies and lawful directions
- Immediately report any suspected misuse or security issue

Limited personal use may be permitted provided it:

- Does not interfere with work duties
- Does not incur cost to Echo Interpreting
- Does not breach any policy or law

6. Use of Personal Devices (BYOD)

Personal devices may be used for work purposes only where:

- They are password-protected and secure
- Confidential information is not stored unnecessarily
- Screens are not visible to unauthorised persons
- Devices are not shared with others while logged in

Users must not:

- Store Echo Interpreting data on unapproved cloud services
- Leave devices unattended in public places
- Use unsecured public Wi-Fi for sensitive work

Workers using personal devices for Echo Interpreting work must take reasonable steps to protect work-related information stored, accessed, or transmitted through those devices.

Workers may be required to securely delete Echo Interpreting information from personal devices when it is no longer required or when their employment or engagement ends.

7. Information Security and Data Protection

Echo Interpreting is committed to protecting business, client, participant, worker, and confidential information from unauthorised access, disclosure, misuse, loss, or interference.

All workers must take reasonable steps to protect information accessed, stored, or transmitted when performing work for Echo Interpreting.

All workers must:

- Protect usernames, passwords, and access credentials
- Not share login details or allow unauthorised access to Echo Interpreting systems
- Use strong passwords and multi-factor authentication where available
- Ensure devices used for work purposes are appropriately secured
- Keep devices, applications, and software reasonably up to date
- Lock devices or log out of systems when not in use
- Store and share information using approved systems where possible
- Only access information required for their role or assigned work
- Report suspected security incidents, unauthorised access, or information breaches as soon as practicable

Workers must not intentionally access, copy, download, modify, delete, disclose, or share Echo Interpreting information unless authorised and required for legitimate work purposes.

All information must be managed in accordance with Echo Interpreting's **Privacy & Confidentiality Policy** and **Privacy & Data Breach Procedure**.

8. Email, Messaging and Digital Communication

When using email or messaging platforms for Echo Interpreting work, users must:

- Communicate professionally and respectfully
- Ensure recipients are authorised before sharing information
- Ensure communications involving client matters remain professional and appropriate
- Use approved systems where possible

Confidential information must not be shared via:

- Personal social media messaging
- Unsecured or informal platforms
- Group chats where recipients are not authorised

9. Online Interpreting and Remote Services

Workers providing services through online or video platforms must:

- Maintain confidentiality during remote assignments
- Ensure conversations cannot reasonably be overheard
- Use appropriate professional environments where practicable
- Protect client and assignment information
- Comply with professional standards and Echo Interpreting requirements

10. Social Media Use

Echo Interpreting recognises that workers may use social media in a personal capacity. However, online conduct must not compromise professionalism or confidentiality.

Users must not:

- Identify clients, assignments, or case details
- Share images, videos, or stories relating to work
- Comment publicly on clients, colleagues, or stakeholders
- Present themselves as speaking on behalf of Echo Interpreting without authorisation

Personal social media activity must not:

- Breach confidentiality
- Damage Echo Interpreting's reputation

- Harass, bully, or discriminate against others

11. Monitoring and Access

Echo Interpreting reserves the right to:

- Monitor use of its systems where lawful and reasonable
- Access business records and communications as required
- Restrict or revoke system access where appropriate

Monitoring will be conducted in a proportionate and lawful manner.

12. Security Incidents and Breaches

Echo Interpreting is committed to identifying, responding to, and managing actual or suspected information security incidents promptly and appropriately.

A security incident may include:

- Loss or theft of a device containing Echo Interpreting information
- Unauthorised access to systems, accounts, or information
- Accidental disclosure or sharing of confidential information
- Emails, messages, or information sent to the incorrect recipient
- Suspected hacking, malware, phishing, or unauthorised activity
- Loss, alteration, or misuse of personal, client, participant, worker, or business information

All actual or suspected security incidents, privacy breaches, or unauthorised disclosures must be reported as soon as practicable in accordance with Echo Interpreting's **Privacy & Data Breach Procedure** and **Incident / Near Miss Reporting Procedure/Form**.

Echo Interpreting will:

- Assess and respond to reported incidents
- Take reasonable steps to reduce potential harm
- Implement corrective actions where required
- Review incidents to identify opportunities for improvement
- Notify affected individuals, organisations, regulators, or authorities where required by law

13. Breach of Policy

Failure to comply with this policy may result in:

- Removal of system access
- Removal from assignments
- Disciplinary action

- Termination of employment or engagement
- Referral to external authorities where appropriate
- Legal action where appropriate

The seriousness of the response will reflect the nature and impact of the breach.

14. Related Documents

This policy must be read and applied in conjunction with:

- Code of Conduct Policy
- Privacy & Confidentiality Policy
- Privacy & Data Breach Procedure
- Incident / Near Miss Reporting Procedure/Form

15. Policy Acknowledgement

All workers are required to acknowledge that they have read, understood, and agree to comply with this Policy.