IT Usage Policy

Introduction

Beanies Family Support Pty Ltd, based in Huon Valley, Tasmania, is committed to leveraging information technology (IT) to enhance service delivery and operational efficiency. Our services include Child and Young Person Advocacy, NDIS Application Support, NDIS Support Coordination, Youth Coaching, Early Intervention Support, Early Childhood Service Consulting, Counselling, and Community Event Support. This IT Usage Policy outlines the standards and procedures for the appropriate use of IT resources to ensure consistency, quality, and security.

Purpose

The purpose of this policy is to:

- Define the standards for the use of IT resources within Beanies Family Support Pty Ltd.
- Ensure the secure and efficient use of IT systems.
- Outline the responsibilities of staff, volunteers, and contractors regarding IT usage.
- Establish procedures for accessing, using, and managing IT resources.
- Protect the integrity, confidentiality, and availability of IT systems and data.

Scope

This policy applies to all Beanies Family Support Pty Ltd staff, volunteers, contractors, and Board members who use the organisation's IT resources.

IT Usage Principles

1. Appropriate Use

IT resources should be used primarily for work-related purposes that support the mission and objectives of Beanies Family Support Pty Ltd. Personal use of IT resources should be limited and must not interfere with work responsibilities or the operation of IT systems.

2. Security

The security of IT systems and data is paramount. Users must take all reasonable precautions to protect IT resources from unauthorised access, viruses, malware, and other security threats.

3. Confidentiality

Users must ensure that sensitive and confidential information is protected at all times. This includes adhering to data protection policies and using secure methods for storing and transmitting information.

4. Compliance

All use of IT resources must comply with relevant legislation, organisational policies, and ethical standards. This includes respecting intellectual property rights, privacy laws, and the organisation's code of conduct.

5. Responsibility

Users are responsible for their actions while using IT resources. This includes maintaining the integrity of IT systems, reporting security incidents, and using resources in a manner that reflects the organisation's values and professional standards.

Responsibilities

1. Board of Directors

The Board of Directors is responsible for overseeing the implementation of this IT Usage Policy and ensuring compliance with relevant legislation and standards.

2. Executive Director

The Executive Director is responsible for ensuring that effective IT systems and procedures are in place and that staff are trained in their responsibilities.

3. IT Manager

The IT Manager is responsible for the day-to-day management of IT resources, including system maintenance, security, and user support. The IT Manager ensures that IT resources are used in accordance with this policy.

4. Staff and Volunteers

All staff and volunteers are responsible for adhering to the IT Usage Policy and procedures. They must ensure that IT resources are used appropriately and securely, and report any IT-related issues or incidents promptly.

Procedures

1. Accessing IT Resources

- Authorization: Access to IT resources is granted based on job roles and responsibilities. Users must obtain appropriate authorization before accessing systems and data.
- User Accounts: Unique user accounts are assigned to each individual. Users must not share their account credentials and must use strong passwords that are changed regularly.
- Remote Access: Remote access to IT systems is permitted for authorised personnel using secure methods, such as VPNs, to ensure data protection.

2. Using IT Resources

- Software and Applications: Only authorised software and applications may be installed and used on organisational devices. Users must not install unauthorised or pirated software.
- Internet and Email Use: Internet and email resources must be used responsibly. Users must avoid accessing inappropriate websites, sending offensive emails, or engaging in activities that could harm the organisation's reputation or IT systems.
- Data Storage: Sensitive data must be stored securely on designated servers or cloud services. Personal devices should not be used to store organisational data unless authorised and secured.

3. Security Measures

- Antivirus and Anti-Malware: All devices must have up-to-date antivirus and anti-malware software installed. Regular scans should be performed to detect and remove threats.
- Software Updates: Users must ensure that all software and operating systems are kept up to date with the latest security patches.
- Backup: Regular backups of critical data must be performed to prevent data loss. Backups should be stored securely and tested periodically to ensure their integrity.

4. Reporting and Incident Management

- Incident Reporting: Users must report any IT security incidents, such as data breaches, malware infections, or unauthorised access, to the IT Manager immediately.

- Incident Response: The IT Manager is responsible for managing IT incidents, including containment, investigation, and resolution. Users must cooperate with incident response procedures and provide necessary information.

5. Monitoring and Compliance

- System Monitoring: The use of IT resources is subject to monitoring to ensure compliance with this policy. Monitoring activities are conducted in accordance with privacy laws and organisational guidelines.
- Compliance Audits: Regular audits are conducted to assess compliance with IT usage policies and procedures. Findings from audits are used to improve IT security and resource management.

6. Training and Awareness

- Staff Training: All staff and volunteers must receive training on IT usage policies, security practices, and their responsibilities. Training is provided during onboarding and through regular refresher sessions.
- Ongoing Awareness: Regular updates and reminders are provided to maintain awareness of IT security issues and best practices.

Implementation and Review

This IT Usage Policy will be reviewed annually or as required by changes in legislation or organisational needs. The Board of Directors and senior management are responsible for ensuring the policy is effectively implemented and adhered to by all staff and volunteers.

Conclusion

Beanies Family Support Pty Ltd is committed to maintaining the highest standards of IT usage to support the secure and efficient delivery of services. By adhering to the principles and procedures outlined in this IT Usage Policy, we aim to ensure the proper management and protection of IT resources, enabling us to provide consistent and reliable services to our clients and the community in Huon Valley.