ALBANY STUDENTS' ASSOCIATION
Representing Students
ASA.AC.NZ

Policy Title	ASA Computer Use Policy
Last Review Date	September 2020
Next Review Date	September 2021
Effective Date	8/9/20

ASA Computer Use Policy

Contents

1. Purpose and Scope

This policy provides guidelines for the use of Association computer network and associated devices and services. The policy sets boundaries for use of Association equipment and internet services. The policy applies to all users of ASA's computer services.

2. Network

ASA's computing requirements are managed using an in-house server with a NAS (Network Attached Storage) drive.

All Windows based devices will be installed with Windows 10 and connect to ASA's domain to ensure that they receive the appropriate security policies.

3. Device Allocation

Staff members will be allocated the necessary computing devices (and associated software) to carry out their roles. This shall usually include a laptop, docking device and additional screens as relevant to the role.

All Association devices are to be returned to the Association at the end of any employment agreements.

The President and Vice-President will each be allocated a laptop for the duration of their term of office. The laptop must be returned to the Association at the end of their term of office.

The other executive team members will be able to access the ASA server using their individual credentials to sign into a shared computer in the ASA office.

Mobile devices, e.g. tablets, smartphones may be made available for events and social media purposes.

4. Data Security

Other than in exceptional circumstances, staff will only engage in Association matters on approved Association devices. All documents are to be stored on the shared NAS drive and should not be permanently stored on the local computer. It is accepted that in some situations work may be carried out on the local computer, but it is imperative that the file is reinstated on the NAS at the earliest opportunity. (e.g. large design files, problem with VPN.

The President and Vice-President should only engage in Association matters on their approved Association device. Executive who do not have an Association device, should conduct all Association business using the facilities provided by their Office365 subscription and documents should be stored in their OneDrive folder or other Association storage.

All Association laptops are BitLocker encrypted. BitLocker will be managed, and keys stored in the central Active Directory for security purposes.

All Association laptops must have up to date anti-virus software.

Association devices are not for personal use and no personal data is to be stored on any Association device or shared network storage.

Association devices may not be used for any other business purposes other than to conduct the business of the Association.

To mitigate privacy risks, Association documents are **not** to be stored on personal computers, unless in an exceptional circumstance. Where this is the case, they are to be removed from the personal computer as soon as the emergency is resolved, and they have been saved back to Association storage. This does not apply to Association documents that are in the public arena, e.g. available from the ASA website.

Only Association IT support and general manager will have administration passwords that will allow software to be installed on Association laptops.

5. Passwords

Passwords need to be changed regularly to ensure data security.

Staff passwords are to be changed every 180 days.

Executive passwords are to be changed on an annual basis or when a new executive member takes office.

Passwords must be at least 7 characters long and must include at least one uppercase character, one lowercase character and one number.

Passwords will be centrally managed.

Only Association IT support and general manager may be allocated administrator passwords.

6. Website

ASA's website is hosted by an external provider. Weekly backups of the ASA website and associated databases are stored on the ASA NAS.

Staff are provided with access to website backend services as appropriate to their roles.

7. Email

Microsoft Office 365 will be used to provide email services.

Each staff member and executive member will be provided with an email account.

ASA email accounts are also provided to each affiliated club.

Association email accounts are to be used for Association business purposes only and personal email accounts should not be used for Association business purposes.

The Association may use a bulk email provider to send emails to its membership provided the member has opted into receiving these communications.

Recipients of bulk email sent either by the Association or by the University on behalf of the Association must be given the opportunity to unsubscribe from the mailing list.

8. Data Backup

Association data is backed up at least daily to an external USB drive and to OneDrive.

Association website databases are backed up weekly to the ASA NAS.

9. VPN – Offsite Access

VPN software is installed on Association laptops to facilitate offsite access to the shared network files.

10. Internet Use

Staff and executive will be entitled to use the internet for reasonable personal use, but this should be limited to periods outside of working hours and must meet the ethical and social standards of the workplace.

No user may download, send, or store material that would be considered illegal, offensive, or inappropriate, this could include but is not limited to pornography, unlicensed music, movies, videos, or software.

Internet usage can be monitored, and breaches will be reported to the general manager.

The Association reserves the right to contract an external consultant to undertake periodic spot checks on individual computer systems and servers to ensure compliance of this policy.

11. Software Licences

Only software approved by the Association IT support or general manager may be installed on Association devices.

Where software is protected by a licencing agreement any violation of the licencing agreement is not allowed.

12. Network Drives and Storage

The Association's shared network drive is set up so that staff and executive only have access to the folders relevant for them to perform their roles.

Data should only be held in a single location, i.e. there should not be multiple copies of the same document filed across the network.

13. Data Retention

Constitutionally the Association is bound to keep and preserve all records likely to prove of value or historic interest.

Data pertaining to Association accounts must legally be held for a minimum of 7 years.

Personal information pertaining to Advocacy services will be held for 3 years.

14. References

- Human Rights Act 1993
- Privacy Act 1993
- Film, Video and Publications Act 1993
- Copyright Act 1994
- Unsolicited Electronic Messages Act 2007
- Health and Safety at Work Act 2015
- Harmful Digital Communications Act 2015