GOV – IT Policy

Policy

Our aim at Headway Gippsland is to ensure that all data is safely and securely stored with appropriate storage of backups.

This policy sets out the minimum standards that must be adhered to by all staff of Headway Gippsland Inc. This policy is available to all staff at Headway Gippsland.

IT Equipment and responsibilities

The organisation maintains the following computer system:

A main server in the Morwell office that is replicated to the servers in the Drouin and Newborough offices.

The servers are connected together via site-to-site VPN's

All the workstations are networked and have internet access.

The main server is in Morwell and replicates to the Servers in Newborough and Drouin.

All software installation files are downloaded from the cloud (Microsoft 365).

Access to this server and its relevant software is restricted to Glenn Reynolds of Edcomp IT Services.

The IT company, Edcomp IT Services is responsible for:

- maintaining the system and liaison with IT contractors or technicians when necessary
- providing advice to the organisation regarding IT issues
- providing an IT orientation to new staff members
- providing IT support to staff

Backup

The server in Morwell office is automatically backed up to the cartridge in the external cartridge dock every working day at 5.30pm.

The external cartridge dock (180mm x 110mm) sits in the server bay

Each morning, the cartridge should be ejected and placed in the safe. To eject the cartridge from the external cartridge dock, press the eject button on the dock. The second cartridge which was already in the safe should now be inserted in the external cartridge dock ready for the evening backup.

Weekly, a representative from Headway will return the cartridge dock to Edcomp and exchange for the cartridge stored at Edcomp, so long as it is the latest backup. If the latest backup is still in the external cartridge dock, then that cartridge should be sent for offsite storage.

In the event that the cartridge is not swapped, the next backup will still work and NOT overwrite the previous version. The cartridge stores many backups and only starts overwriting the oldest when full. It is the responsibility of Administration to regularly swap the cartridges, and return to EdComp

If the cartridge is required to restore the server, a technical support resource from Edcomp will identify the latest backup and implement the recovery.

Users

- All users of IT at Headway Gippsland must be registered users. The Administration Office will organise registration and initial password allocation.
- At first logon, the new user will be directed to change the temporary password to a password of their choosing. The password needs to be complex, include a mixture of alphabetical characters, numbers at least one capital and at least 1 special character, e.g., @, #, % etc. Passwords must be a minimum of 8 characters.
- Passwords are to be changed frequently, with 3 months the maximum period between password updates.
- Passwords MUST not be shared. Passwords must remain CONFIDENTIAL.
- Any laptop or mobile phone will be returned to EdComp to have data removed once an employee has left Headway Gippsland, emails forwarded onto relevant staff
- Certificate of Destruction issued or information transferred to a new machine to be issued by EdComp
- If IT equipment is no longer required by the organisation, it must be destroyed in such a way that data cannot be retrieved from that equipment. All Surplus IT, equipment is cleaned and held securely at EdComp, A Certificate of Destruction issued or information transferred to a new machine to be issued by Edcomp
- **Network**
- Current, respected antivirus software will be in place on all devices and all patches with antivirus updates will be installed automatically, without delay.
- The servers will have enabled firewall protection with intrusion detection and prevention tools enabled.
- Operating systems will be kept updated and all security patches applied at the earliest opportunity.
- The server will be backed up not less than daily and a weekly backup kept offsite with our IT support organisation.
- Incident logs are retained for all down times and unsuccessful attempts to breach security.
- Our systems also allow privilege settings to ensure client information, particularly, is available on a need-to-know basis.
- Our internal wireless services use WPA2 encryption.

- Initial user ids and passwords for System Admin purposes are renamed.
- The IT support contractor and the Headway Gippsland management team will regularly audit the implementation and maintenance of the IT security standards to ensure full compliance
- The organisation has a clean screen and clean desk policy with auto log-offs for dormant users and shredding of all sensitive documents when they are updated or periodically reviewed

Information Management and access

Access levels are restricted to

Level 1: CEO Group

Level 2: Executive Team

Level 3: Management Team

Level 4: Support coordination team

Level 5 Plan Management Team

Level 6: Finance

Level 7: Client Services

Level 8: Marketing and Communications

Level 9 : Administration

Access Level		
1. Forms	All levels	
2. Policies	All levels	
3. Handbooks	All levels	
4. Registers	Level 1, 2, 3	
5. Master Documents	Level 1, 2, 3	(Sub-folders of Forms, Policies, Handbooks)
6. Archived Documents	Level 1, 2, 3	(Sub-folders of Forms, Policies, Handbooks, Registers)
7. Employees – Exec	Level 1	
8. Employees - Office	Level 1, 2, 6	
9. Employees – LSO's	Level 1, 2, 3, 6	(Sub-folders for each employee in the format Surname, First name + Archived Employees)

Workplace Surveillance

Headway may at any time carry out surveillance and monitoring such as, but not limited to:

- Conduct computer surveillance of all its information technology systems, including email usage, internet usage and any other usage of information technology supplied by Headway. This surveillance is carried out on a continuous and ongoing basis and will be ongoing from the commencement of your employment.
- Camera surveillance by way of closed-circuit television cameras. The surveillance is continuous and ongoing. For the purposes of your employment with Headway and exposure to the surveillance, it effectively starts upon your commencement. Access to the recorded material will be strictly limited to authorised personnel.
- Tracking surveillance of its vehicles by means of an electronic device the primary purpose of which is to monitor or record geographical location or movement (such as a Global

  Positioning System tracking device). This surveillance is carried out on a continuous and ongoing basis and will be ongoing from the commencement of your employment.
- Tracking surveillance of its electronic devices (e.g., smartphones, tablets, computer equipment) by means of an electronic device the primary purpose of which is to monitor or record geographical location or movement (such as a Global Positioning System tracking device). This surveillance is carried out on a continuous and ongoing basis and will be ongoing from the commencement of your employment.
- Access to email accounts owned by Headway and provided for employee use.

Headway may use the surveillance records for any purpose, including purposes related to your employment or the employment of other company employees or contractors. You may consult with the company about the surveillance at any time. For the purposes of discussing any queries or comments about the company's surveillance activities, please contact your manager.

You consent to this surveillance.

Use of internet

Use of the organisation's computer network to access the internet for personal use is permitted, provided it conforms to the organisation's policy on personal use of organisational resources.

This prohibits use of the network to:

- access pornographic, gambling or gaming related sites or material
- use eBay or similar online purchasing sites or 'dating' sites
- create or exchange messages, images or sounds that are offensive, harassing, defamatory, obscene, sexually harassing or threatening
- download any files without permissions for intellectual property rights (including commercial software, games, music or movies)
- create or exchange advertisements, solicitations, chain letters and other unsolicited or bulk email
- download software without the approval of the Executive Team
- play games in work time – unless in allocated break times
- Staff should also ensure that any activity on a personal social network site does not identify or implicate Headway Gippsland in any way and that organisational policies regarding confidentiality and privacy are extended to all internet exchanges.

Cyber Security

Procedures

Prepare : Headway Gippsland have implemented

- Increased awareness to staff about potential risks
- Multi factor authentication

Prevent :

- Multifactor authentication
- Alert set up for emails outside of the organization.
- Advise Edcomp of any suspicious emails when an alert is received
- Restrictive administration privileges are in place
- Auto Patch Operating system
- Daily back up and monthly back up by Edcomp
- Microsoft office macros disabled

Respond: A breach response consists of four steps: Contain, Assess, Notify & Review Headway Gippsland will:

- Immediately notify the CEO and Edcomp to confirm the breach has occurred. Once confirmed
- Depending on the nature of the breach.
- The following will be considered as the most appropriate action by Edcomp
    - Stopping the unauthorized practice
    - Recovering the records
    - Shutting down the system that was breached
    - Changing computer access

Assess the risks of harm to the affected individuals by investigating the circumstances of the breach

- Headway Gippsland will take into consideration Whether and how to notify affected individuals, Notification may not be appropriate if it is reasonably likely to cause more harm than it would alleviate.
- Notify Office of the Victorian Information Commissioner (OVIC) of incidents involving personal information that could cause harm to affected individuals by accessing the following website with online form

https://incident-notifications.ovic.vic.gov.au/

Consequences of a Data Breach

Harm to individuals as a result of a data breach can be physical, financial, emotional or reputational. Some examples of harm arising from a data breach include:

- Reputational damage
- Embarrassment or humiliation
- Emotional distress
- Identity theft or fraud
- Financial Loss
- Disruption of services

Headway Gippsland could also suffer harm as a result of a data breach. Responding to the initial breach

And subsequent complaints may have financial, legal and resource implications. Furthermore, data breaches can result in reputational damage and loss of public trust.

Further information can be sought at

https://cyber.gov.au/