IT USE POLICY

1. Purpose

This policy sets out guidelines for the use of our IT systems.

2. Application

This policy applies to all of Name of company employees, anyone who performs work for us, anyone who performs work on our premises and anyone who uses our IT systems (referred to collectively in this policy as "employees").

This policy applies to all use of our IT systems.

3. What are IT systems?

IT systems mean all of our information technology, computing and communications systems and equipment. This includes but is not limited to:

- hardware such as computers, laptops, tablets, landline phones, mobile phones, printers, scanners, monitors, projectors, audio-visual systems, video conferencing systems, cameras and security systems;
- software, operating systems, web browsers, computer programs, computer files and databases;
- email systems;
- anything that enables access to the internet, websites, internet domain names, IP addresses, intranet systems and extranet systems;
- telecommunications systems and voicemail systems;
- networks, network equipment, servers, storage and archive systems.

4. Use of IT systems

- Employees may only use our IT systems for legitimate business purposes and limited personal use.

- Employees must ensure that all use of our IT systems is done in the best interests of our business and is not detrimental to our business in any way.

- Employees must comply with our workplace policies when using our IT systems, including our Code of Conduct and Workplace behaviour and respect policy.

5. Security

- Employees must comply with all directions with respect to the security of our IT systems that are made from time to time.

- Employees must not allow any other person to access or use our IT systems unless they are authorised to do so. This includes family or household members when work is being done at home.

- Employees must use secure passwords and not share their passwords with any other person.

- Employees are responsible for maintaining the security of all portable technology, such as laptops, tablets and mobile phones. Employee are required to use locks and passwords on all portable technology to ensure that each item is kept secure at all times.

- Employees must immediately notify us if there is any loss or damage to portable technology so we can assess whether any security measures need to be taken.

- Employees must not use our IT systems to access any data for which they are not the intended recipient or do not have authority to access, unless doing so is a usual part of their duties.

- Employees must not log into any server or account that they are not expressly authorised to access, unless it is part of their regular duties.

- Employees must not install any unauthorised software on our IT systems. If an employee believes that access to a certain application is required for their work, they should contact the IT team.

6. Use of the internet

- Use of the internet should be primarily for business purposes with limited personal use.
- All use of the internet must comply with our workplace policies, including our Code of Conduct and Bullying, Harassment and Discrimination policy.
- Employees must not access websites that contain obscene, hateful, pornographic, violent or illegal material.
- Employees must not post, upload or download any material that:
    - is illegal;
    - is obscene, pornographic or violent;
    - contains discriminatory, harassing or threatening messages or images; or
    - is defamatory in any way;
    - contains hate speech or racist material, racial epithets or religious bigotry.

7. Email use

- Our email system must only be used by people who have been granted access and who have been issued an email and password.
- Employees must not disclose their email passwords to any other person.
- Employees must not allow any other person to use their email account.
- Email is to be used primarily for business purposes with limited personal use.
- Employees must exercise care when opening attachments received from non-company sources.
- Any files downloaded from emails received from non-company sources must be scanned with our virus protection software. Any virus, tampering or systems problems should be immediately reported.

- All email use must comply with our Code of Conduct and Bullying, Harassment and Discrimination policy.

- Employees must not send unsolicited email messages, such as junk mail or advertising material, to anyone who has not specifically requested it.

- All emails sent or received using our IT systems are our property. We may monitor, access, read, disclose and use any email without prior notice to the sender or recipient of the email. Email communications using our IT systems are not private.

8. Confidential information

- Our IT systems must not be used to disclose, transmit, copy or remove confidential information without authorisation to do so.

- Employees must take all steps necessary to ensure our IT systems are not used to disclose, transmit, copy or remove confidential information without authorisation.

- Employees must promptly notify us if they become aware of any use of our IT systems to disclose, transmit, copy or remove confidential information.

9. Unacceptable use of IT systems

Employees must never use our IT systems to:

- access material that is obscene, hateful, pornographic, violent or illegal;

- send, post, upload or download any material that:

    - is illegal;

    - is obscene, pornographic or violent;

    - contains discriminatory, harassing or threatening messages or images; or

    - is defamatory in any way;

    - contains hate speech or racist material, racial epithets or religious bigotry;

- perpetrate any form of fraud or other illegal activity;

- violate the rights of any person with respect to the protection of privacy, confidential information, copyright, trademarks, patents or any other intellectual property rights;

- engage in film or music piracy, including by downloading or copying software or electronic files without authorisation;

- engage in unauthorised copying, digitization or distribution of photographs from magazines, books or other copyrighted sources;

- install, duplicate, acquire or use software in a manner that is not accordance with software copyrights and licenses;

- make fraudulent offers of products, items or services;

- introduce malicious programs into our network (such as viruses, worms, trojan horses, email bombs, etc);

- send or post information that may harm our business, its products or services, our employees, clients or customers.

10. Surveillance of IT systems

We will conduct surveillance of all use of our IT systems. The surveillance will be continuous and ongoing.

We will carry out the surveillance by all means available to us, which will include but is not limited to:

- using monitoring software to monitor access and use of our computer systems;

- maintaining and accessing the records that are ordinarily created by using our IT systems;

- auditing, logging, monitoring and accessing email accounts, emails sent and received, draft emails, instant messaging and voicemail;

- maintaining and accessing records of internet use, including websites visited and for how long, files downloaded or uploaded, video and audio files accessed and data input;

- accessing any files stored on our IT systems;

- accessing work computers, laptops, tablets, phones or other electronic devices used by employees, including any files or other information stored on them;

- maintaining and accessing logs, backups and archives of email, network and internet use.

We may use and disclose computer surveillance records or information obtained as a result of computer surveillance for any legitimate purpose related to the employment of our employees or our legitimate business activities or functions. This includes, but is not limited to, managing IT security, conducting workplace investigations and taking disciplinary action against employees.

11. Breaches of this policy

An employee who breaches this policy may be subject to disciplinary action up to and including termination of their employment.

Application of this policy

If any part of this policy is contrary to law the law will apply to the extent of the inconsistency.

This policy is subject to review by us and may be changed or revoked at any time.

If an employee has a valid reason for not complying with this policy, they should contact management so management can consider whether to grant an exception.

Need more information?

Contact People	HR Contact Email: hr@greystanes.org.au
Version Number	1.0
Review Details	This policy is effective from 17th January 2025 This policy was last updated on 17th January 2025

(Annexure A)

Procedure for Responding to an IT Security Breach

This document outlines the steps to be taken by the organisation in the event of an IT security breach to effectively manage the situation, contain damage, and prevent future occurrences.

This procedure applies to all employees, contractors, and partners of Greystanes Disability Services who use or manage the company's information systems and data.

Procedure Steps:

Detection and Identification:

- Monitor systems for unusual activity using intrusion detection systems (IDS), security information, and event management (SIEM) systems.
- Employees should immediately report any suspected security incidents to the Business Operations Manager.

Initial Response:

- Once a potential security breach is reported or detected, the designated security officer or IT personnel must assess the scope and impact.
- If a breach is confirmed, initiate the incident response plan by assembling the incident response team.

Containment:

- Disconnect affected systems from the network to contain the breach.
- Preserve evidence by taking images of the affected systems.
- Document all steps taken, including the date and time of actions.

Eradication:

- Identify and remove the root cause of the breach.
- Update security patches and strengthen firewall rules.
- Change passwords and access control credentials.

Recovery:

- Restoring systems from clean backups and ensuring they are not compromised before reconnecting to the network.
- Gradually return systems to operational status under strict monitoring for any signs of malicious activity.

Notification:

- Notify internal stakeholders, including executive management, legal, and public relations teams.
- As per the data breach notification laws in your jurisdiction, promptly inform affected clients, partners, and users.
- If necessary, report the breach to the relevant authorities.

Post-Incident Analysis:

- Conduct a thorough investigation to understand the breach's causes and implications.
- Document lessons learned and update the incident response plan accordingly.

Remediation Measures:

- Implement additional controls to prevent future breaches.
- Conduct regular security training for employees.
- Schedule periodic audits and assessments to reinforce security posture.

Reporting and Documentation:

- Prepare a comprehensive breach report for internal use and, if necessary, for regulatory bodies.
- Maintain records of the breach investigation and recovery process as per compliance requirements.

Responsibility:

- All employees are responsible for reporting suspected security incidents.
- The IT department is responsible for investigating and responding to security breaches in coordination with other departments.

Review and Testing:

- This procedure must be reviewed annually or in response to significant changes in the IT environment or after a breach incident.
- Regular testing of the incident response plan should be carried out to ensure its effectiveness.