



Data Protection Policy

Company Policy No: 11SA
Company: Greencastle Solutions Ltd
Issue No: 2
Revision Date: April 2026
Review Date: April 2027

Data Protection Policy

1 Policy Objective

- 1.1 This policy describes the company's guidelines regarding access to and disclosure of both direct and indirect electronic messages sent or received by employees with use of the company's electronic communication system.
- 1.2 While the company respects the individual privacy of its employees, employee privacy does not extend to the employee's work-related conduct or to the use of company-provided equipment or supplies. All employees should be aware that the guidelines herein might affect their privacy in the workplace.
- 1.3 In all circumstances, the use of all telephonic as well as direct/indirect electronic mail messages or communications by employees shall be considered and regarded as and for business use only.

2 Application

This policy applies to all company employees.

3 Company Communication Systems/Facilities

- 3.1 For the purposes of this policy, company communication systems/facilities are seen as including but not limited to the following:
 - 3.1.1 The company's electronic mailing system as well as its domain.
 - 3.1.2 The company's intranet, Employee Self-Service, or any internal network system.
 - 3.1.3 Any 3G/4G/LTE/Wi-Fi/LAN/Ethernet or any other internet access provided by the company.
 - 3.1.4 Any mobile device, personal computer or laptop provided by the company.
 - 3.1.5 Any other system/facility.

4 Right to Access of Information

- 4.1 The electronic communications system has been installed to facilitate business communications. Although each employee has an individual password to access this system, it belongs to the company and the contents of direct and indirect communications are always accessible by management for any business purpose.
- 4.2 These systems may be subject to periodic unannounced inspections and should be treated in the same manner as other shared filing systems.

- 4.3 All system passwords and encryption keys must be available to company management, and employees may not use passwords that are unknown to their supervisors or install encryption programs without turning over encryption keys to the supervisor.
- 4.4 All electronic correspondence is considered company record. The contents of communications, properly obtained for legitimate business purposes, may be disclosed within the company without an employee's permission. Therefore, employees should not assume that messages are confidential.
- 4.5 Back-up copies of communications may be maintained and referenced for business and legal reasons.

5 Personal use of Email and Communication Systems

- 5.1 Because the company provides the communication system to assist employees in the performance of their duties, they should use it for official company business only.
- 5.2 While incidental and occasional personal use is permitted, these messages will be treated in the same manner as other business messages. The company reserves the right to access and disclose as necessary all messages sent over its communication system, without regard to content.
- 5.3 Since personal messages can be accessed by management without prior notice, employees should not use company systems to transmit any messages that they would not want read by a third party e.g. emails should not be used for gossip, including personal information about yourself or others, for forwarding messages under circumstances likely to embarrass the sender, or for emotional responses to business correspondence or work situations.
- 5.4 In any event, employees should not use these systems for purposes such as soliciting or advertising for commercial ventures, religious, or personal causes or outside organisations or other similar, non-job-related solicitations.
- 5.5 If management discovers misuse of the communication system, the offender will be subject to disciplinary action up to and including termination of the employment contract once due process has been followed.

6 Password and Encryption Key Security and Integrity

Employees are prohibited from the unauthorised use of passwords and encryption keys of other employees to gain access to other employees' email messages.

7 Corporate Company Guideline

- 7.1 Acceptable uses of the internet and company communication systems:
 - 7.1.1 Every staff member has a responsibility to maintain and enhance the company's public image and to use company email and internet access in a productive manner. To ensure that all employees are responsible, the guidelines herein have been established for using email and the internet.

- 7.1.2 Company-provided internet and email access is intended to be for business use only. While the company encourages the use of the internet and email to make communication more efficient and effective, both are company property, and their purpose is to facilitate company business.
- 7.1.3 Any improper use of the internet or communication systems is not acceptable and will not be permitted.

7.2 Unacceptable uses of the internet and company communication systems:

- 7.2.1 Company email and internet access may not be used for transmitting, retrieving, or storing any communications of a discriminatory or harassing nature, or materials that are obscene or pornographic.
- 7.2.2 Access to and receipt of any pornographic material of any nature whatsoever is strictly prohibited.
- 7.2.3 Employees may not use the company communication systems in any way that may be seen as insulting, disruptive, or offensive to other persons, or harmful to morale. Examples of forbidden transmissions include sexually explicit messages, cartoons or jokes, unwelcome propositions, love letters, derogatory or inflammatory remarks, ethnic or racial slurs, any other message that can be construed to be harassment or disparagement of others based on, inter alia, their sex, race, disability, sexual orientation/preference, age, national origin, religious or political beliefs, or physical attributes.
- 7.2.4 No abusive, profane, or offensive language is to be transmitted through the company's email or internet system.
- 7.2.5 Electronic media may also not be used for any other purpose which is illegal or against company policy or contrary to the company's best interests.
- 7.2.6 Solicitation of non-company business or any use of company email or internet for personal gain is prohibited.
- 7.2.7 Use of company-provided communication systems that is in any manner in violation of this guideline will result in disciplinary action and shall be considered a dismissible offence.

7.3 Communications:

- 7.3.1 Each employee is responsible for the content of all text, audio, or images that they place or send over the company's communication systems. No email or other electronic communications may be sent which hides the identity of the sender or represents the sender as someone else or someone from another company. All messages communicated on the company's email/internet system should contain the employee's name.
- 7.3.2 Any messages or information sent by an employee to another individual outside of the company via an electronic network (e.g. bulletin board, online service, or internet) are statements that reflect on the company. While some users include personal 'disclaimers' in electronic messages, there is still a connection to the company, and the statements may be tied to the company.
- 7.3.3 All communications sent by employees via the company's communication systems must comply with this and other company policies, may not disclose any confidential or proprietary company information, and shall always be subject to the level of authority of the employee concerned to transact for and on behalf of the company.
- 7.3.4 The company shall not accept any liability of the employee for any communication to third parties in breach of this policy as such communication shall be considered and regarded to be outside of the course and scope of the employee's normal duties with the company. The employee shall also be subject to disciplinary action in such an event.

7.4 Software:

- 7.4.1 To prevent computer viruses from being transmitted through the company's communication and information systems, no unauthorised downloading or any unauthorised software shall be permitted.
- 7.4.2 All downloaded software must be registered to the company.
- 7.4.3 Employees should contact management if they have any questions in this regard.

7.5 Copyright issues:

- 7.5.1 Employees may not use the company's communication systems to transmit copyrighted materials belonging to entities other than this company. All employees obtaining access to other companies' or individuals' materials must respect all copyrights and may not copy, retrieve, modify, or forward copyrighted materials, except with permission, or as a single copy for reference purposes only. Failure to observe copyright or license agreements may result in disciplinary action up to and including termination of the employment contract.

7.6 Security:

- 7.6.1 The company routinely monitors usage patterns of its electronic communications for various reasons including cost analysis/allocation and managing the company's internet gateway. All messages created, sent, or retrieved over the company's communication systems are the property of the company and should be considered public information.
- 7.6.2 The company reserves the right to access and monitor all messages and files on the company's communication systems.
- 7.6.3 Employees should not assume that electronic communications are totally private and should transmit highly confidential data by any alternative means.

7.7 Virus protection:

- 7.7.1 All employees are to ensure that their computer is enabled with the company-approved virus protection software.
- 7.7.2 Computer viruses are a real threat, and they should be treated as such. It is the responsibility of each employee to ensure that any media introduced into the company computer is free from any virus. No program(s) may be introduced onto the company computers without permission from the relevant manager/network supervisor.
- 7.7.3 The above is valid for any computer program of whatever nature whether introduced by external media or via a network or the internet/intranet.
- 7.7.4 To effectively protect its assets against virus attacks, the company reserves the right to open or dispose of any email sent or received by employees (private or otherwise). Company management reserves the right to block or delete any incoming and/or outgoing email that it regards as a risk.

7.8 Computer games:

- 7.8.1 The company does not allow the playing of computer games on the company's computers as this may affect productivity in the workplace.
The company's computers are provided for company use only. Usage for personal and private business activities is therefore prohibited and may only be conducted with the permission of the relevant manager.

8 Policy Breach

- 8.1 Any employee who abuses the privilege of company-facilitated access to the communication system, internet, or intranet, will be subject to corrective action up to and including termination of the employment contract.

- 8.2 If necessary, the company also reserves the right to advise appropriate legal officials of any illegal activities by offenders.