

IT Security and Communication Policy

[Name of the Company](#) believes a clear communication policy reduces conflicts and misunderstandings. Organizations also need to state clearly how electronic equipment and facilities may be used, so as to avoid liability and trouble. This policy covers IT usage and communication.

Purpose

This policy sets out what the organization expects and manages how communication flows, both inside and outside the organization.

It aims to support meaningful, essential communication that helps employee productivity and morale, without restricting communication so much that employees feel intimidated or powerless.

Scope

This policy applies to all employees of the company.

Guiding Principles

[Name of the Company](#) recognizes that active communication with stakeholders and the general public is a core part of its strategy. To meet its communication goals, employees must follow these guidelines:

- Only authorized people may hold formal meetings with external stakeholders, including media engagements and press releases.
- All information must reach [Name of the Company](#)'s stakeholders on time, through appropriate, approved channels.
- All stakeholder requests for information get a turnaround of [Number of days](#) working days.
- Information given to stakeholders must be accurate, transparent and as open as possible, while [Name of the Company](#)'s confidentiality is maintained.
- All communication must be clear, concise and purposeful.
- Feedback is collected regularly from all of [Name of the Company](#)'s stakeholders to improve service delivery.

Guidelines for External Communication

The support and engagement of external stakeholders are critical to [Name of the Company](#)'s long-term success. All communication with them should support that, and aim to keep stakeholders well informed and not confused.

- All external communication must be approved by [Formal Title of the Person](#) and routed through [Formal Title of the Person](#). Communication with government representatives, and the sharing of other confidential information, needs approval from [MD or CEO](#).
- [Formal Title of the Person](#) must review all presentations and materials used externally before they reach stakeholders, including those for meetings, seminars and conferences and anything uploaded.
- Communication with the media must be handled with great sensitivity and professionalism, and always directed by [Formal Title of the Person](#).

Guidelines for Internal Communication

- [Name of the Company](#)'s internal communication is aimed at all internal stakeholders and supports the company's overall objectives.
- The teams responsible for internal correspondence handle it.
- Communication between staff must always be professional.
- Address staff by first name in speech and by initials in writing. Official letters must use the staff member's full name.
- Nicknames or other names are strictly forbidden in written communication.

Disclosure of Confidential Information

- [Name of the Company](#) is committed to timely, accurate and complete disclosure of necessary company information, in an appropriate manner.
- [Name of the Company](#) strictly prohibits the disclosure of confidential information.
- Employees must sign a Non-Disclosure and Confidentiality Agreement. Violating it is a legal offense.

Information Security and Monitoring Policy

This policy gives a combined set of security measures that must be applied consistently across [Name of the Company](#) to guarantee a secure operating environment for its business.

It covers the information security requirements of confidentiality, integrity and availability.

Electronic and Wireless Policy

[Name of the Company](#) has this policy to keep its data and technology infrastructure safe.

Employees should protect personal and company-issued devices with passwords and keep anti-virus software up to date.

Employees must log in only over secure networks.

Cell Phone Policy

This policy applies to any device that can make or receive calls, leave messages, send texts, browse the internet, download information, and view and answer email, whether it is owned personally or by the company.

Company-owned cell phones must stay switched on during working hours, work-related travel, and any other times the company specifies.

Employees must not use cell phones:

- While driving
- While operating equipment
- During meetings
- For long personal calls during office hours
- For recording the company's confidential information

Employees can use cell phones for:

- Making business-related calls
- Checking important messages
- Scheduling or checking appointments
- Short personal calls

[Name of the Company](#) has the right to monitor inappropriate or excessive cell phone use. Disciplinary action will be taken if these terms are breached.

Internet Usage Policy

The electronic communication system must be used only for company business.

Employees are warned against using the internet for personal advantage or entertainment.

Employees should be aware that content they create has no right to privacy and can be used by the company without prior notice.

Appropriate use means using the internet to complete assigned work and to find information for it.

Internet use is inappropriate if an employee uses it to:

- Upload or download obscene, illegal or offensive material
- Expose the company's confidential information to unauthorized parties
- Invade other employees' privacy
- Engage in piracy
- Visit unsecured websites that threaten the safety of the computer network
- Hack

A breach of this policy makes the employee liable to disciplinary or legal action.