Information Technology

General

This employee internet usage policy applies to our employees, contractors, volunteers and partners who access our network and computers.

Employees are advised to use the office internet connection for the following reasons:

- To complete their job duties.
- To seek out information that they can use to improve their work.
- To access their social media accounts, while conforming to our social media policy.

While the Yoma Group does not want to restrict our employees' access to websites of their choice, but we expect our employees to exercise good judgment and remain productive at work while using the internet. Any use of our network and connection must follow our confidentiality and data protection policy.

Employees should:

- Keep their passwords secret at all times.
- Log into their corporate accounts only from safe devices.
- Use strong passwords to log into work-related websites and services.

Employees should not use the network to:

- Download or upload obscene, offensive or illegal material.
- Send confidential information to unauthorized recipients.
- Invade another person's privacy and sensitive information.
- Download or upload movies, music and other copyrighted material and software.

Visit potentially dangerous websites that can compromise the safety of our network and computers.

Perform unauthorized or illegal actions, like hacking, fraud, buying/selling illegal goods and more.

Employees are also advised to be careful when downloading and opening/executing files and software. If they're unsure if a file is safe, they should ask their supervisor or IT helpdesk.

Anti-virus and disk encryption software may be installed on the Yoma Group's computers. Employees may not deactivate or configure settings and firewalls without managerial approval.

The Yoma Group shall not be responsible if employee devices are infected by malicious software, or if their personal data are compromised as a result of inappropriate employee use.

Company-issued equipment

Employees are expected to respect and protect any equipment belonging to the Yoma Group. "Company equipment" in this computer usage policy for employees includes company-issued phones, laptops, tablets and any other electronic equipment, and belongs to our company.

Employees are also advised to lock their devices in their desks when they're not using them, and remain responsible for their any Company equipment whenever taken out of the offices.

Email

Employees may use their corporate email accounts for both work-related and personal purposes as long as they don't violate this policy's rules. Employees shouldn't use their corporate email to:

- Register to illegal, unsafe, disreputable or suspect websites and services.
- Send obscene, offensive or discriminatory messages and content.
- Send unauthorized advertisements or solicitation emails.
- Sign up for a competitor's services unless authorized.

The Yoma Group has the right to monitor corporate emails. And the right to monitor websites employees visit on any Company equipment.

Disciplinary Action

Employees who do not comply with this employee internet usage policy will face disciplinary action. Serious violations will be cause for termination of employment, or legal action when appropriate. Examples of serious violations are:

- Using our internet connection to steal or engage in other illegal activities.
- Causing our computers to be infected by viruses, worms or other malicious software.
- Sending offensive or inappropriate emails to our customers, colleagues or partners.

Company Data Protection Policy

This policy is applicable all parties (including employees, job applicants, customers, suppliers, contractors etc.) who provide information to the Yoma Group. As part of our operations, the Yoma Group may need to obtain and process information. This information includes any offline or online data that makes a person identifiable such as names, addresses, usernames and passwords, digital footprints, photographs, social security numbers, financial data etc.
The Yoma Group will collect this information in a transparent manner and with the full cooperation and knowledge of interested parties.

The Yoma Group will ensure that the personal data be:

- Collected fairly and for lawful purposes only
- Processed by the company within its legal and moral boundaries

- Protected against any unauthorized or illegal access by internal or external parties

Any personal data will not be:

- Communicated informally
- Stored for more than a specified amount of time

Transferred to organizations, states or countries that do not have adequate data protection policies.

Distributed to any party other than the ones agreed upon by the data's owner (exempting legitimate requests from law enforcement authorities)

In the collection of personal information, the Yoma Group also undertakes to:

- Inform people that their data is collected
- Inform people about how data is processes
- Have provisions in case of lost, corrupted or compromised data

Allow people to request that any data provided in relation to themselves be modified erased, reduced or corrected in the databases.

Actions

The Yoma Group will:

- Restrict and monitor access to sensitive data
- Develop transparent data collection procedures
- Train employees in online privacy and security measures
- Build secure networks to protect online data from cyber attacks
- Establish clear procedures for reporting privacy breaches or data misuse
- Include contract clauses or communicate statements on how we handle data
- Establish data protection practices (document shredding, secure locks, data encryption, frequent backups, access authorization etc.)

Disciplinary Consequences

All principles described in this policy must be strictly followed. A breach of data protection guidelines will invoke disciplinary and possibly legal action.