

Email Policy

1. Purpose and Scope

This policy protects company data, keeps communication professional, and reduces legal, security and operational risk. It applies to all employees, contractors, consultants, interns and temporary staff, and covers every email account the company provides. Follow it whenever you use company email.

2. Acceptable Use

Company email is for work. Messages should relate to your job and support company objectives. Accounts are provided for:

- Internal team communication
- Communication with clients, vendors and partners
- Scheduling meetings
- Sharing work-related documents
- Receiving company-approved newsletters and industry updates

3. Inappropriate Use

Anything that puts security, compliance or the company's reputation at risk is prohibited. Do not use company email for illegal, unethical or non-work activity, including:

- Gambling, illegal downloads or copyright violations
- Harassment, hate speech, discrimination or offensive language
- Sending inappropriate jokes, images or content that could offend others
- Running a personal business or side venture
- Misrepresenting your identity, authority or job role

4. Personal Use

Management may restrict or prohibit personal use of company email. Do not use it for financial subscriptions or sign-ups. Where limited personal use is allowed, it must be:

- Minimal and occasional
- Not disruptive to work
- Not harmful to system performance or security

5. Email Security Requirements

Everyone must follow company security standards, including strong passwords and multi-factor authentication. In particular:

- Never share your email credentials.
- Be careful with unknown emails, links and attachments.
- Watch for phishing and spoofed emails.
- Use approved encryption or secure file-sharing methods when required.

Report any suspected security incident to the IT or security team immediately, as set out in the Email Security Policy.

6. Data Protection and Confidentiality

Protect confidential and sensitive company information, and always check that the recipient is authorized to receive it. That means:

- Do not send company data to personal email accounts.
- Do not share information with unauthorized recipients.

7. Email Etiquette and Professional Conduct

Every email sent from the company domain represents the organization. You are expected to:

- Keep a respectful, professional tone.
- Write clear subject lines.
- Use approved email signatures.
- Reply within expected timelines, based on urgency.

8. Email Retention, Backup and Monitoring

Company emails are official business records and may be accessed during company audits or legal investigations. Do not treat your inbox as personal storage.

9. Consequences of Non-Compliance

Serious violations, such as data leakage, harassment or deliberate security breaches, may lead to immediate termination and legal action.