# Email Acceptable Use Policy

To use this template, simply replace the text in dark grey with information customized to your organization. When complete, delete all introductory or example text and convert all remaining text to black prior to distribution.

|  |  |
| --- | --- |
| **Policy Owner** | Name the person/group responsible for this policy’s management. |
| **Policy Approver(s)** | Name the person/group responsible for implementation approval of this policy. |
| **Related Policies** | Name other related enterprise policies both within or external to this manual. |
| **Related Procedures** | Name other related enterprise procedures both within or external to this manual. |
| **Storage Location** | Describe physical or digital location of copies of this policy. |
| **Effective Date** | List the date that this policy went into effect. |
| **Next Review Date** | List the date that this policy must undergo review and update. |

# Purpose

Describe the factors or circumstances that mandate the existence of the policy. Also state the policy’s basic objectives and what the policy is meant to achieve.

Email is a critical mechanism for business communications at [Company Name]. However, use of [Company Name’s] electronic mail systems and services are a privilege, not a right, and therefore must be used with respect and in accordance with the goals of [Company Name].

The objectives of this policy are to outline appropriate and inappropriate use of [Company Name’s] email systems and services in order to minimize disruptions to services and activities, as well as comply with applicable policies and laws.

# Scope

Define to whom and to what systems this policy applies. List the employees required to comply, or simply indicate “all” if all must comply. Also indicate any exclusions or exceptions i.e. those people, elements or situations that are not covered by this policy or where special consideration may be made.

This policy applies to all email systems and services owned by [Company Name], all email account users/holders at [Company Name] (both temporary and permanent), and all company email records.

# Definitions

Define any key terms, acronyms or concepts that will be used in the policy. A standard glossary approach is sufficient.

# Governing Laws & Regulations

If applicable, list any laws or regulations that govern the policy or with which the policy must comply. Confirm with the legal department that the list is full and accurate. If there are no pertinent governing laws or regulations, delete this section.

# Policy Statements

Describe the rules that comprise the policy. This typically takes the form of a series of short prescriptive and proscriptive statements. Sub-dividing this section into sub-sections may be required depending on the length or complexity of the policy.

1. Email access at [Company Name] is controlled through individual accounts and passwords. Each user of [Company Name’s] email system is required to read and sign a copy of this email acceptable use policy prior to receiving an email access account and password. It is the responsibility of the employee to protect the confidentiality of their account and password information.
2. All employees of [Company Name] will receive an email account. Email accounts will be granted to third-party non-employees on a case-by-case basis. Possible non-employees that may be eligible for access include:
* Contractors
* [Insert category]
* [Insert category]

Applications for these temporary accounts must be submitted to [insert contact name and contact information]. All terms, conditions, and restrictions governing email use must be in a written and signed agreement.

1. Email access will be terminated when the employee or third party terminates their association with [Company Name], unless other arrangements are made. [Company Name] is under no obligation to store or forward the contents of an individual’s email inbox/outbox after the term of their employment has ceased.
2. [Company Name] often delivers official communications via email. As a result, employees of [Company Name] with email accounts are expected to check their email in a consistent and timely manner so that they are aware of important company announcements and updates, as well as for fulfilling business and role-oriented tasks.
3. Email users are responsible for mailbox management, including organization and cleaning. If a user subscribes to a mailing list, he or she must be aware of how to unsubscribe from the list, and is responsible for doing so in the event that their current email address changes.
4. Email users are expected to remember that email sent from the company’s email accounts reflects on the company. Please comply with normal standards of professional and personal courtesy and conduct.
5. Email users are not to give the impression that they are representing or providing opinions on behalf of [Company Name] unless otherwise authorized.
6. Email users will not forward emails to accounts outside the control of [Company Name].
7. Individuals at [Company Name] are encouraged to use email to further the goals and objectives of [Company Name]. The types of activities that are encouraged include:
* Communicating with fellow employees, business partners of [Company Name], and clients within the context of an individual’s assigned responsibilities.
* Acquiring or sharing information necessary or related to the performance of an individual’s assigned responsibilities.
* Participating in educational or professional development activities.
1. [Company Name’s] email systems and services are not to be used for purposes that could be reasonably expected to strain storage or bandwidth (e.g. emailing large attachments instead of pointing to a location on a shared drive). Individual email use will not interfere with others’ use and enjoyment of [Company Name’s] email system and services.
2. Email use at [Company Name] will comply with all applicable laws, all [Company Name] policies, and all [Company Name] contracts. Use in a manner that is not consistent with the mission of [Company Name], misrepresents [Company Name] or violates any [Company Name] policy is prohibited.
3. The following activities are deemed inappropriate uses of [Company Name] email systems and services, and are strictly prohibited. Inappropriate use includes, but is not limited to:
* Use of email for illegal or unlawful purposes, including copyright infringement, obscenity, libel, slander, fraud, defamation, plagiarism, harassment, intimidation, forgery, impersonation, soliciting for illegal pyramid schemes, and computer tampering (e.g. spreading of computer viruses).
* Use of email in any way that violates [Company Name’s] policies, rules, or administrative orders, including, but not limited to, [list any applicable code of conduct policies, etc.].
* Viewing, copying, altering, or deletion of email accounts or files belonging to [Company Name] or another individual without authorized permission.
* Sending of unreasonably large email attachments. The total size of an individual email message sent (including attachment) should be [insert size in KBs] or less.
* Opening email attachments from unknown or unsigned sources. Attachments are the primary source of computer viruses and should be treated with utmost caution.
* Sharing email account passwords with another person, or attempting to obtain another person’s email account password. Email accounts are only to be used by the registered user.
* Excessive personal use of [Company Name] email resources. [Company Name] allows limited personal use for communication with family and friends, independent learning, and public service so long as it does not interfere with staff productivity, pre-empt any business activity, or consume more than a trivial amount of resources. [Company Name] prohibits personal use of its email systems and services for unsolicited mass mailings, non-[Company Name] commercial activity, political campaigning, dissemination of chain letters, and use by non-employees.
1. The email systems and services used at [Company Name] are owned by the company, and are therefore its property. This gives [Company Name] the right to monitor any and all email traffic passing through its email system. This monitoring may include, but is not limited to, inadvertent reading by IT staff during the normal course of managing the email system, review by the legal team during the email discovery phase of litigation, observation by management in cases of suspected abuse, or to monitor employee efficiency.
2. Archival and backup copies of email messages may exist, despite end-user deletion, in compliance with [Company Name’s] records retention policy. The goals of these backup and archiving procedures are to ensure system reliability, prevent business data loss, meet regulatory and litigation needs, and to provide business intelligence.
* Backup copies exist primarily to restore service in case of failure. Archival copies are designed for quick and accurate access by company delegates for a variety of management and legal needs. Both backups and archives are governed by the company’s document retention policies. These policies indicate that email must be kept for up to [xx] years. [Replace with details of retention policy.]
1. If [Company Name] discovers or has good reason to suspect activities that do not comply with applicable laws or this policy, email records may be retrieved and used to document the activity in accordance with due process. All reasonable efforts will be made to notify an employee if his or her email records are to be reviewed. Notification may not be possible, however, if the employee cannot be contacted, as in the case of employee absence due to vacation.
2. Use extreme caution when communicating confidential or sensitive information via email. Keep in mind that all email messages sent outside of [Company Name] become the property of the receiver. Consider not communicating anything that you wouldn’t feel comfortable being made public. Demonstrate particular care when using the “Reply All” command during email correspondence to ensure the resulting message is not delivered to unintended recipients.
3. Any allegations of misuse should be promptly reported to [insert name of contact and contact information]. If you receive an offensive email, do not forward, delete, or reply to the message. Instead, report it directly to the individual named above.
4. [Company Name] assumes no liability for direct and/or indirect damages arising from the user’s use of [Company Name’s] email system and services. Users are solely responsible for the content they disseminate. [Company Name] is not responsible for any third-party claim, demand, or damage arising out of use the [Company Name’s] email systems or services.

# Non-Compliance

Clearly describe consequences (legal and/or disciplinary) for employee non-compliance with the policy. It may be pertinent to describe the escalation process for repeated non-compliance.

Violations of this policy will be treated like other allegations of wrongdoing at [Company Name]. Allegations of misconduct will be adjudicated according to established procedures. Sanctions for non-compliance may include, but are not limited to, one or more of the following:

1. Temporary or permanent revocation of e-mail access;
2. Disciplinary action according to applicable [Company Name] policies;
3. Termination of employment; and/or
4. Legal action according to applicable laws and contractual agreements.