

[This sample can be used to design your own policy, keeping in mind the specific environment in which you work and the expectations of the senior leaders of the company]

Scope of this Policy

The company provides services (such as email and CMS systems) computers and network connected printers for the sole purpose of conducting company business. Personal use is not allowed of these devices. The company does provide a 'guest' network and a printing service for personal use, however, privacy is not to be expected when using this network or printing service so that we may monitor usage and ensure it stays in compliance with these policies.

Employee Responsibilities

- Company-provided desktops and networked printers can only be used for conducting company business.
- Files received by email will be scanned by our email system and that process should be allowed to complete.
- Violations of these policies, even unintentional, should be communicated to senior staff.

Unacceptable Use

- Company-provided services and equipment (including internet access, guest network access and personal printing services) should not be used in ways that are disruptive, offensive, harassing, discriminatory or abusive. This includes viewing or distributing disruptive, offensive, harassing, discriminatory or abusive materials.
- Employees may not forward messages of a religious or political nature, sexually explicit content, chain letters, solicitations or other inappropriate usage.
- Employees may not engage in illegal activities using company-provided services and equipment (including internet access, guest network access and personal printing services)
- Employees may not install their own software or plugins, even if they have a personal license for it. Any software installations must be pre-approved by senior management.
- Employees must not divulge their passwords, even to IT staff.

Administration of this Policy

- The company provides safeguards through a variety of means (email filters, anti-virus scanning, access control policies, etc.)
- Regular audits are performed by IT staff in addition to automated system alerts.
- Network traffic and equipment use is monitored and employees should have no expectation of privacy, even when using the guest network.
- Violations of this policy could result in disciplinary action up to and including termination.