

Electronic Resources Policy

Policy statement

3M's electronic resources provide many tools through which information can be shared around the globe. The efficient use of electronic resources contributes to 3M's success. It is 3M policy that the company's electronic resources be used only in ways that do not violate the law, 3M's Business Conduct Policies or 3M Information Policies. 3M employees must also protect 3M electronic resources from unauthorized uses and security threats.

The term "3M electronic resources" means all electronic devices, software, systems and networks, directly or through a third party, used to transmit, receive, process or store 3M information or data. 3M electronic resources include, but are not limited to, computers, servers, databases, PDAs, telephones, wireless devices, e-mail systems, voice messaging systems, and Internet connectivity. It also includes the use of non-3M-owned electronic resources storing or connecting to 3M data. This policy applies whenever and wherever 3M electronic resources are accessed and used.

3M allows reasonable and limited personal use of 3M electronic resources by employees. Employee personal use must be occasional and brief, must not unduly burden 3M's resources and systems, must comply with all laws and 3M policies, and must not interfere with normal business activities or the employee's ability to meet job expectations. In addition, employee personal use for outside business ventures, personal financial gain is prohibited. Except as permitted by the [3M Political Activities Policy](#), use of 3M electronic resources for political purposes also is prohibited.

3M reserves the right to monitor or access employee communications or other materials created, received, stored, transmitted or processed using 3M's electronic resources, at any time and without notice, where there is a business reason to do so and as permitted by law. For this reason, users of 3M's electronic resources should not have an expectation of privacy in e-mails, documents, files, voice files or other communications or materials created, received, stored, transmitted or processed using 3M electronic resources, unless required by law.

What it means

- Use 3M electronic resources in accordance with 3M policies and applicable laws, including 3M policies and laws regarding information security, [Confidential information](#), [Regulated information](#), privacy, harassment, political activities, software implementation and record retention.
- Take appropriate measures to protect the security, confidentiality and integrity of 3M electronic data and information, as required under 3M policies and applicable laws. For example:
 - Protect User IDs (UPINs) and passwords for 3M electronic resources and ensure their proper use. Passwords are confidential information.
 - Ensure that your workstation and mobile devices connecting to 3M networks meet corporate standards. Do not uninstall or disable 3M-provided security

solutions, such as anti-virus tools, firewalls or password-protected screensavers.

- Lock workstations when left unattended.
 - If using 3M electronic resources in public places, take appropriate measures to protect 3M confidential information. For example, when using your laptop computer on airplanes or in hotel lobbies, use a supported privacy screen filter.
 - Use only properly licensed copies of computer software. Do not copy or use software licensed to 3M unless 3M's license from the software publisher permits the copying or use.
- Limit your personal use of 3M electronic resources. Make sure your use is occasional and brief, does not unduly burden 3M's resources and systems, complies with all 3M policies, and does not interfere with normal business activities or your ability to meet job expectations.
- Be aware that 3M reserves the right to access and monitor 3M electronic resources and employee use of those resources, as permitted by law.

What to avoid

- Using electronic resources in a manner that violates any law or 3M Business Conduct Policy.
- Using electronic resources in a manner inconsistent with a respectful business environment or which violates [3M's Harassment Policy](#), for example, by sending offensive or harassing messages or downloading or viewing sexually explicit or other offensive material.
- More than occasional, brief personal use of 3M electronic resources.
- Using 3M electronic resources for outside business ventures or personal financial gain.
- Downloading, copying or using software or other materials in violation of copyright laws or license restrictions.
- Posting a list of passwords next to your workstation.
- Disabling any 3M-required software.
- Using the 3M email system to send personal photos or other large non-business files, which can negatively impact 3M network operations.