



ELECTRONIC RESOURCES PRINCIPLE

Principle Statement :

GTG employees and third parties to whom this Principle applies must protect GTG electronic resources from unauthorized uses and security threats, and must not use GTG's electronic resources for outside business ventures or personal financial gain. Personal use of electronic resources must be reasonable, limited, and may not interfere with GTG's normal business activities or an employee's ability to meet job expectations.

GTG reserves the right to monitor or access employee or third party communications or other materials created, received, stored, transmitted, or processed using GTG's electronic resources, at any time and without notice, where there is a business reason to do so and as permitted by law and applicable regulations and agreements in the respective group company. For this reason, users of GTG's electronic resources should not have an expectation of privacy in emails, documents, files, voice files or other communications or materials created, received, stored, transmitted, or processed using GTG electronic resources, including when using GTG's electronic resources for personal use in accordance with this Principle, unless required by law or guaranteed in applicable regulations and agreements in the respective group company.

Purpose :

GTG's electronic resources provide many tools through which information can be shared around the globe. The efficient use of electronic resources contributes to GTG's success. To safeguard and protect GTG's property and resources, GTG's electronic resources must be used lawfully and in a manner that complies with GTG's policies and procedures.

This Principle applies globally to all employees and may apply to those acting on behalf of GTG. See the Compliance Principle for information on when a third party might be covered by the Code of Conduct Principles.

Additional Guidance :

- The term "GTG electronic resources" means all electronic devices, software, systems, and networks, directly or through a third party, used to transmit, receive, process or store GTG information or data. GTG's electronic resources are for GTG business. These resources include, but are not limited to, computers, mobile phones, servers, databases, wireless devices, tablets, email systems, voice messaging systems, remote access tools and internet connectivity. It also includes the use of non-GTG-owned electronic resources that store or connect to GTG data. This Principle applies whenever and wherever GTG electronic resources are accessed and used.
- Use GTG electronic resources in accordance with GTG policies and agreements or regulations in the respective group company and applicable laws, including GTG policies and laws regarding information security, confidential information, regulated information, privacy, harassment, political activities, software implementation and record retention.
- Never use electronic resources in a manner inconsistent with a respectful business environment or which violates GTG's Respectful Workplace Principle, for example, by sending offensive or harassing messages or downloading or viewing sexually explicit or other offensive material.
- Take appropriate measures to protect the security, confidentiality, and integrity of GTG electronic data and information, as required under GTG policies and applicable laws. For example:
 - Protect User IDs and passwords for GTG electronic resources and ensure their proper use. User IDs and passwords are confidential information. Never post them near the computer; record IDs/passwords in a secure manner.





ELECTRONIC RESOURCES PRINCIPLE

Additional Guidance :

- Ensure that workstations and mobile devices connecting to 3M networks meet corporate standards. Do not uninstall or disable GTG-provided security solutions, such as anti-virus tools, firewalls, or password-protected screensavers.
- Lock workstations when left unattended.
- When using GTG's electronic resources in public places, protect GTG confidential information, for example, by using a privacy screen and being aware of surroundings.
- Use only properly licensed copies of computer software. Do not copy or use software licensed to GTG unless GTG's license from the software publisher permits the copying or use.
- Do not download, copy, or use software or other materials in violation of intellectual property laws or license restrictions.
- GTG allows reasonable and limited personal use of GTG computers, mobile phones and other personal devices for email and internet browsing by employees and other permitted users. Any personal use must not unduly burden GTG's resources and systems, must comply with all laws and GTG policies regulations and agreements in the respective group company, and must not interfere with normal business activities or the employee's ability to meet job expectations. Any personal use remains subject to the principle set out above that users of GTG's electronic resources should not have an expectation of privacy unless required by law or guaranteed in applicable regulations and agreements.
- Employee personal use of GTG electronic resources for personal financial gain, such as in connection with outside business ventures or personal financial gain is prohibited.
- Except as permitted by the GTG Lobbying and Political Activities Principle, use of GTG electronic resources for political purposes (for example, campaigning or fundraising in connection with a political party or election for public office) is prohibited.
- Never use the GTG email system to send or upload personal photos or videos or other large non-business files that can negatively impact GTG network operations.
- Employees reporting possible information security incidents or violations of this Principle should report the incident to the IT Helpline, GTG-Ethics.com, their assigned legal counsel, or any of the resources listed in the Employee Obligations and Reporting Principle.

Penalties:

A variety of laws and regulations apply to the use of GTG electronic resources, including, but not limited to, software licensing, systems security, business use of the internet (including laws relating to unsolicited commercial email), data privacy, deceptive advertising, harassment, and unfair competition laws. Failure to comply with these laws could lead to criminal and civil penalties for GTG and for employees personally, significant business disruptions, and harm to GTG's reputation. Violations of GTG's Code of Conduct will result in discipline, up to and including termination from employment.

