

GEPE agreement on use of electronic communication systems

Preamble

Internet, intranet and use of e-mail can add considerably to fast communication and effective provision of information. Therefore the company provides these tools to all employees to maximally free disposal. Through the worldwide circulation and the possibility of anonymous use Internet contains, however, also the danger of the abuse, also in legal respect. If these tools are improperly used, it can expose both GE (the “company”) and individual users to liability for antitrust and/or copyright violations for improper receipt, downloading or dissemination of information. In addition, GEP must continue to protect trade secrets and proprietary information that could be improperly disseminated internally or externally through e-mail or the internet.

This agreement gives employees guidelines for the correct use of electronic communication systems such as e-mail and the Internet. Moreover, this agreement gives guidelines to prevent and/or react to violations of this policy.

As this agreement is supposed to be used for all European sites of the company, all local legislation will be taken into account. In case any part of this agreement is in conflict with any applicable local and/or European legislation, the latter prevails. Data protection and privacy Directives of the EU are referred to.

Guidelines for correct use of electronic communication systems

1. Use of the telephone, the internet, intranet, and e-mail are to be used for work-related purposes. Occasional private use is permitted, provided that the work is not affected, no additional costs for the company arise and legislation, ethical standards and GE integrity policies are respected. This means that company computer resources may, in any event, not result in misuse of work time.

2. Examples of illegal and/or inappropriate use are:

- Participating in on-line gambling or “chain letters” or accessing or disseminating pornographic material is strictly prohibited.
- Sending messages with sexual content/overtones or messages that would tend to disparage or harass others on the basis of gender, race, age, disability, religion, sexual orientation or national origin.

(These are *examples* of prohibited use of electronic communications. This list is not meant to be exhaustive.)

3. Moreover, employees should bear in mind that electronic communications must be written, communicated and stored in a manner consistent with all other applicable GEP policies. For example:

- GEP document retention policy, procedures and schedules. All electronic communications are subject to the GEP document retention policies. If an electronic communication needs to be stored in order to comply with established document retention or litigation document preservation requirements, it should be printed by the originator or recipient and placed in the appropriate file.
- Company policy 20.5. The internet’s enormous capacity for accessing and distributing information may raise concerns regarding compliance with company policy 20.5. As internet use expands, so does the likelihood of increasing contacts with competitors and access to

sensitive competitive information. The antitrust compliance principles outlined in company policy 20.5 are applicable to all information available through e-mail, the internet or other electronic communication systems.

4. Last but not least, the following rules apply:

- Employees may disclose electronic communications or information contained in electronic communications only to authorised employees. This is especially important with respect to legal and proprietary information. Therefore, posting confidential or proprietary information regarding the company, its products or its customers on unsecured internet sites, such as bulletin boards, is strictly prohibited.
- All computer-based communications containing technical or proprietary information must be marked "Company confidential & proprietary."
- Employees may not download or distribute copyrighted material available through computer networks without proper authorisation and/or payment of applicable fees.
- Employees may not use company computer communication systems to solicit on behalf of outside business interests or charitable organizations without first receiving written approval from their manager and the GEP legal operation.
- Employees may not download, use or distribute software or executable programs from computer networks without first verifying their operational integrity, ie the absence of computer viruses, etc.

Guidelines to prevent and react to violations of this agreement:

1. In order to prevent abuse of the internet as far as possible, the company has installed an internet-filter and will maintain or instal new filters when needed. Installation of a new type of filter however, will only take place after having consulted the EWC and/or local works council. This filter contains the web addresses of internet sites with inappropriate content. Attempts to access such sites are rejected and strictly prohibited. Instead of the referred internet site the user receives a message that the access to this site is prohibited.

2. In cases where illegal and/or inappropriate use is suspected (eg voluntary introduction of viruses, paedophilia, attempts to access inappropriate sites, occurrence of e-mails with inappropriate content or attachments), management has a justified reason to investigate and monitor the e-mail and internet usage of suspected data subjects. In the event applicable law and regulations prohibit such, management or employee may request an investigation by external consultants.

3. Violation of any of the foregoing rules and guidelines may result in discipline up to and including discharge.

4. For backup purposes, copies of e-mail files may be made automatically and kept for three months. In case management has reasons to keep copies any longer, the local works council will be informed.

Agreement signed in October 2002 by GEPE management and EWC.