

LEICA MICROSYSTEMS, INC.

ELECTRONIC COMMUNICATIONS POLICY

Scope of Policy

This document sets forth the policies of Leica Microsystems, Inc. ("Leica") regarding the use of its electronic communications systems ("systems"), which include but are not limited to electronic mail, voice mail, facsimiles, computers and related equipment, the intranet, and the Internet and the World Wide Web. All those who use Leica's systems agree by such use to comply with the rules outlined in this Policy. Use of Leica's systems is a privilege that may be revoked in Leica's sole discretion, and one that automatically terminates upon your departure from Leica.

Ownership of Information and Employee Responsibility

Leica's systems and all information stored on them are Leica property. All information and messages that are created, sent, received, accessed, or stored using Leica's systems constitute Leica records. Leica owns all information on its systems as well as all information related to Leica business stored on your own personal computer. Upon employment, each individual permitted to use Leica's computer network becomes responsible for protecting the resources and data over which he or she has control. This includes protection of physical property and electronic data, regardless of how the data is collected or stored. The unauthorized use, modification, or destruction of data or other computing resources is prohibited. Employees must respect the rights of other computer network users. Knowingly accessing or sharing data files without owners permission is prohibited. It is the employee responsibility to report loss of, or damage to, any Leica computer or information. Individual users are also responsible for their own computer files and protecting Leica passwords. Users should not circumvent normal resource limits, logon procedures, or security provisions.

Business Use

Leica's systems are provided at Leica's expense and should be used to conduct Leica business. Your use of Leica's systems should not interfere with the performance of your job or with others' performance of their jobs, should not otherwise interfere with Leica business, and should not otherwise violate this Policy or other Leica policies.

Security of Electronic Communications

Because electronic communications are not inherently secure, you should not send confidential, proprietary, or sensitive information to third parties through e-mail, the Internet, or the World Wide Web without prior authorization from your manager or without first encrypting such messages using Leica-authorized encryption.

No Presumption of Privacy/Leica's Right to Monitor Messages

Communications on Leica's systems are not private. Any passwords or user IDs used to access Leica's systems are designed to

protect Leica's confidential information from outside third parties, not to provide users of Leica's systems with personal privacy in the messages. You should also recognize that all connections and sites you visit in surfing the Internet and World Wide Web may be monitored and recorded. Leica reserves the rights to monitor, access, retrieve, and read all messages created, sent, accessed, received, or stored on Leica's systems without prior notice to the originators and recipients of such messages. Leica may also disclose such messages to law enforcement officials, to other third parties when Leica is legally required to do so, and to third parties and authorized Leica personnel where required for business purposes. Without limitation to the above, Leica also reserves the right to monitor chat rooms and newsgroups, and may examine any material you have uploaded from or downloaded to any of Leica's systems. Leica may at any time monitor, access, retrieve, read, and disclose your electronic communications involving any of Leica's systems under the following circumstances:

- When Leica has a legitimate business need to do so;
- When Leica suspects that a Leica systems user has engaged, or is about to engage, in inappropriate conduct using any of Leica's systems, including violating this Policy or any other Leica policy;
- When required by law, by legal duties to third parties, or in order to protect Leica's own interests; or
- When the Leica systems user in question is unavailable (e.g., ill, on vacation or leave, no longer working for Leica).

Leica reserves the right to keep your e-mail address active for a reasonable period of time following your departure from Leica to ensure that important business communications reach Leica.

Message Restrictions

Communications on Leica's systems may not contain content that a reasonable person would consider to be defamatory, offensive, profane, abusive, obscene, threatening, harassing, disruptive, or derogatory, including but not limited to sexual comments or images, racial or ethnic slurs, or other comments or images that would reasonably offend someone on the basis of race, color, religion, national origin, citizenship status, veterans' status, sex, sexual orientation, marital status, disability, age, or any other characteristic protected by law.

Prohibited Activities

You may not use Leica's systems to:

- Upload, download, or otherwise transmit copyrighted, trademarked, or patented material; trade secrets; or other confidential, private, or proprietary information or materials in violation of the law;
- Upload, download, or otherwise transmit any illegal information or materials, or otherwise engage in any illegal activity;
- Upload, download, access, create, distribute, or otherwise transmit sexually explicit materials;
- Upload, download, access, create, distribute or otherwise transmit materials that advocate violence, hatred, or discrimination toward other people;
- Gain unauthorized access to remote computers or other systems, or damage, alter, or disrupt such computers or systems in any way;
- Use someone else's code or password, or disclose anyone's code or password, including your own;

- Create, distribute, or otherwise transmit chain letters, junk e-mail or faxes, or any other electronic communications that could constitute a nuisance or violate the law;
- Falsify addressing information to conceal the sender's or recipient's identity or otherwise create or distribute anonymous messages;
- Enable unauthorized third parties to have access to or use Leica's systems, or otherwise jeopardize the security of Leica's systems;
- Pass off your views as representing those of Leica or commit Leica to a particular position without appropriate authorization;
- Post information, opinions, or comments to Internet discussion groups, subscriber lists, and other such forums unless such postings are related to a legitimate business activity of Leica; are professional (e.g., must not disparage a competitor or competitor product), accurate, and not contrary to any Leica interests or policy; and do not contain confidential or otherwise inappropriate details about Leica product plans, customers, or technology;
- Additionally, you may not use any non-Leica authorized encryption in connection with any of Leica's systems;
- Send inappropriate jokes or other offensive communications; political causes; football pools or other sorts of gambling; subscription lists for non-Leica purposes; or solicitations or advertisements for non-Leica purposes.

Message Creation

Although electronic communications seem transitory, like a phone call, they are in fact remarkably permanent. Because creating electronic messages is very much like using electronic letterhead that carries your name and Leica's name, you must use great care in creating and transmitting messages on Leica's systems. Even when a message has been deleted, it may still exist on a back-up system, may be recreated, may have been printed out, may have been forwarded to someone else, or may have been viewed by someone other than your intended recipient (whose own e-mail communications may be monitored by an employer, for example). The electronic messages that you are creating today may someday have to be produced by Leica in connection with a lawsuit. Always remember that all of your electronic communications reflect on Leica, despite any disclaimers that you may make.

Record Retention and Deletion

As with paper documents that you create and receive, it is your responsibility to ensure that electronic messages are saved or deleted according to Leica's record retention policies. Any related questions should be directed to your supervisor/manager.

Viruses and Tampering

Any files downloaded from the Internet, attachments to e-mail messages, and computer disks received from non-Leica sources must be scanned with virus detection software before installation, execution, or use. Introduction of viruses, attempts to breach system security, or other malicious tampering with regard to any of Leica's systems are expressly prohibited. You must immediately report any viruses, tampering, or other breaches of any of Leica's systems to your supervisor/manager.

Selling and Purchasing

Leica's standard purchase and sales policies apply to all purchase- and sales-related activities conducted via Leica's systems. Absent permission from your supervisor/manager, you may not use Leica resources to pay Internet/World Wide Web subscription fees or access charges, including but not limited to independent Internet service provider subscription fees.

Violations

Employees should report any violations of this policy to their Supervisor. Violations of this Policy, including breaches of confidentiality or security, may result in suspension of systems privileges and disciplinary action, up to and including termination. To the extent that violations of this Policy may also constitute violations of other Leica policies or various laws, Leica reserves the right to take additional action in accordance with such policies or laws. Leica reserves the right to hold you personally liable for any violations of this Policy.

Leica Electronic Communications Policy

I have read Leica Microsystems, Inc.'s Electronic Communications Policy and agree to abide by it as consideration for my continued employment by Leica Microsystems, Inc. I understand that violation of any above policies may result in my termination.

John Smith

User Name (please print)



User Signature

06/01/2019

Date