UK IT Usage Policy

Purpose

The purpose of the IT Usage Standard is to establish the standard on privacy, confidentiality, and security in electronic communications at Zurich, to ensure that the IT systems and information are used for business purposes, and to prevent the misuse of Zurich IT resources, services, and activities.

- This standard applies to electronic information in all forms used within Zurich, regardless of the format or location in which it is kept.
- This Standard applies to all employees of Zurich and its subsidiaries and affiliates worldwide, and to third-party service providers covered by non-disclosure agreements or contractual obligations.

For the purpose of this standard document:

- Zurich IT Systems means all technical hardware and software resources and tools that are used to create, store, use, share, archive, dispose/delete Zurich information or connect to Zurich IT applications systems.
- Zurich information includes corporate information and information that relates directly or indirectly to our customers, employees, affiliates, partners or any other individuals or organisations with whom we have a relationship.

Responsibilities

You will be required to read, understand and abide by the requirements of Zurich's IT Usage Standard and all associated policies.

Users have a responsibility to promote IT security and to follow the rules of the Global IT Usage Standard. Users must apply all technical and other means provided to them to safeguard the electronic information and systems within their care and use. Users are also accountable for all transactions performed under their user IDs.

Any violation of this Global IT Usage Standard may lead to the termination of the user's access to any or all IT systems and may subject the user to disciplinary action, up to and including termination of employment.

Usage of Information Technology

IT systems provided by Zurich, containing Zurich information, or transmitting Zurich information must be used for the benefit of Zurich. Users are prohibited from using information technology in a manner that will harm or otherwise damage the reputation, integrity or financial position of Zurich or Zurich's IT environment.

Any Zurich information must be stored, handled and transmitted consistent with the Zurich Risk Policy, and the Group Policy 'Protection & Privacy of Personal Data', all of which will be available to you once you join Zurich.

Restriction on Use

IT system users must:

- comply with all relevant rules on data protection, privacy, retention and destruction
- take reasonable steps to ensure the security of Zurich information and equipment
- maintain the individual accountability of each IT system user ID; this includes not permitting another user access to Zurich IT systems using an assigned user ID; each user is accountable for any transaction performed under its user ID
- maintain the secrecy of all IT system passwords; this includes not sharing passwords with anyone including Zurich employees and IT staff
- use passwords that conform to business unit password rules
- not install any software or additional hardware without approval from Group IT
- not disable or change anti-virus or other security software settings or interrupt any security scan of a computer
- not change any predetermined security configuration
- not attempt to gain access to IT system facilities or Zurich information unless authorized to do so.

Personal Use

Reasonable personal use is permitted as long as it does not interfere with business use, is appropriate and is not excessive. Managers are responsible for interpreting what is appropriate and excessive. All personal use must still comply with the user's duty of care.

Privacy

All information, including e-mail messages and files, created, sent, retrieved or backed- up over Zurich IT Systems is the property of Zurich, and should not be considered private or confidential property to the user.

Zurich makes no representations to guarantee the privacy of information operated on Zurich IT Systems except as required by law, regulations, written agreements or Zurich policy.

It is Zurich's policy to respect the privacy of its employees. However, for security, future infrastructure planning, specific site access restriction reasons and checking for compliance to policy, Zurich reserves the right to monitor all activities/communication to and from the Internet through or on its infrastructure.

Zurich may monitor, intercept, review, retrieve, filter, access, audit, store or block any electronic communications or other content on its IT systems, including stored voicemail and e-mail messages, with or without the specific knowledge of the users, as permitted by law, and may do so whether the messages are business-related or personal. Users should be aware that the electronic communication records on their IT systems are discoverable in litigation (e.g., lawsuits, regulatory matters), internal or external research by Zurich, or audit purposes. This includes e-mail, voicemail, text messages, instant messaging conversations, documents, and any other retained communications. Such discovery can be done without the knowledge or consent of the Users.

Internet

Access to the Internet is provided to employees in connection with business purposes. Zurich reserves the sole right to revoke internet access or make any changes as deemed appropriate at any time without any notice, including the disallowing of sites and services. Zurich may limit access to Internet websites and services that are known or expected to contain malicious code, viruses or other threats to the Group's computing environment.

- Access to the Internet from your work laptop or PC is only allowed while connected to the Zurich Network – either directly (e.g. while in the office) or remotely via our approved VPN solution.
- Any data or information that is confidential to Zurich, and it's stakeholders, including but not limited to information on financial information, financial transactions, client information, business plans, business strategies, may not be transmitted through the Internet without appropriate protection.
- Zurich considers infringement of copyright laws to be a criminal act and will treat all incidents as such.
- Access to any site representing but not limited to pornographic, sexual or racial themes or any offence punishable by law is prohibited.
- Participating in chat rooms or any forum not related to business use representing Zurich or otherwise is not allowed.
- Knowingly downloading of any (i.e. getting/bringing) files, material, software, screensavers, wallpaper not for authorised business use on any Zurich notebook, server or PC is prohibited.
- Publishing, distribution or display of any inappropriate, profane, defamatory, infringing, obscene, indecent, pornographic or unlawful material is absolutely prohibited.
- Unauthorised scanning, hacking, testing for security or other weaknesses of any Zurich or non-Zurich system, infrastructure, IT or non-IT related on the Internet and Intranet is absolutely prohibited.
- Only authorised users are permitted to change the default settings of the Internet software configuration on workstations.
- No user is authorised to monitor or maintain their private or any other non-Zurich web sites using Zurich network and/or equipment regardless of it being for a financial gain or not.
- Private use of any of Zurich equipment for conducting personal business for financial gains is prohibited.

E-mail, Messaging, Collaboration

Zurich maintains its e-mail system solely for conducting its business. Copies of messages created, sent, received or stored on the e-mail system are the property of the Company.

Zurich cannot guarantee that electronic communications will be private. Users should be aware that electronic communications could, depending on the technology, be forwarded, intercepted, printed, and stored by others.

Users must use the same care in drafting electronic communication as they would use for any other written communication and as reasonably expected in a professional communication. In particular, users must not use electronic messages to:

- Send chain letters, junk e-mail/messages, spam or any other duplicate electronic messages.
- Defame, abuse, harass, stalk, threaten or otherwise violate the law or legal rights (such as rights of privacy and publicity) of others.
- Conduct business which is not related to official Zurich business.

- Send material that is inappropriate, profane, defamatory, infringing, obscene, indecent or pornographic.
- Knowingly transmit or upload any material that contains software or other material protected by copyright or any material belonging to Zurich except where authorized.
- Knowingly transmit or upload any material that contains viruses, Trojan horses, worms, time bombs, or any other harmful programs or malware.

Social Networking Services (SNS)

Business use of SNS must be authorized by the appropriate Zurich organization, and such use must follow the Zurich Basics code of conduct and other relevant policies and guidelines.

Users must use the same care in using SNS as they would use for any other written communication and as reasonably expected in a professional communication. All employees will be required to read the Social Media Guidelines to ensure they are aware of their responsibilities to Zurich when using social media.

In particular, users must not use SNS to:

- publish Zurich's or others' confidential or other proprietary information. As an exception, it may be appropriate to share such information among a specified group, if purely internal collaboration platforms with restricted access are used
- defame, abuse, harass, stalk, threaten or otherwise violate the law or legal right (such as rights of privacy and publicity) of others
- post content or graphics that are inappropriate, profane, defamatory, infringing, obscene, indecent or pornographic
- knowingly post or upload material that contains software or other material protected by copyright or any material belonging to Zurich except where authorized
- knowingly transmit or upload any material that contains viruses, Trojan horses, worms, time bomb, or any other harmful programs or malware.

Mobile Computing Devices

Mobile devices provided by Zurich and Zurich information on privately owned mobile devices must be used for the benefit of Zurich. Mobile devices that process, store or transmit Zurich information or connect to Zurich systems must be supplied by Zurich or otherwise be approved by appropriate authorities within Group IT.

In addition to all other requirements, mobile computing device users must:

- take reasonable steps to prevent the physical theft of the mobile device or the information stored on it
- report lost or stolen IT systems immediately
- be aware of surroundings and utilize care in the usage of IT systems in public places
- do not permit non-authorized individuals such as family members or others to use Zurich owned equipment.

118623A03 (08/13) ZCA

ZURICH®