

# Replica Ltd

## Information Technology Acceptable Use Policy

Information technology resources are valuable assets provided to facilitate and enable the business activities of Replica Ltd (Replica or the Company). The use of Replica's information technology resources is a privilege extended to authorized users solely in connection with their work for the company. This policy governs the use of Replica's information technology resources.

Information technology in this policy is not restricted solely to the use of computers but includes devices such as mobile telephones, digital cameras and any electronic device owned by the Company.

The Company cannot protect users from the presence of material they may find offensive. The presence of such material must not be represented or construed as an endorsement or approval by the Company.

This policy applies to all staff, customers, and others, referred to as users throughout this policy, while accessing, using, or handling the Company's information technology resources. In this policy, "users" include but are not limited to subcontractors, visitors, contract support personnel, and others who may be granted access. All "users" are required to be familiar with and comply with this policy.

POLICY:

### General Policy

1. All users are expected to act in a responsible, ethical, and lawful manner when using the Company's information technology resources. Users should note that breaches of this acceptable use policy may constitute offences under the Computer Misuse Act 1990 .
2. The Company's information technology resources are provided for use in conducting authorized company business. Using these resources for personal gain, illegal, or obscene activities is prohibited.
3. Minimal personal use of these resources is permitted by this policy, except when such use:
  - Is excessive or interferes with the performance of the user's responsibilities;
  - Results in additional incremental cost or burden to The Company's information technology resources;
  - is otherwise in violation of this policy; or
  - violates any applicable law or regulation.

The use of chat rooms, message boards and instant messaging is unlikely to constitute acceptable use under this policy, unless the user can demonstrate a specific benefit to the Company for each visit or session.

While the Company reserves the right temporarily or permanently to block access to particular web sites, the mere accessibility of a web site does not imply that accessing it is acceptable.

Individual managers may impose further restrictions upon personal use.

4. Users observing any illegal activities should report their observance to the appropriate administrator. Although not an inclusive list, examples include theft, fraud, gambling, copyright infringement, illegal electronic file sharing, sound or video recording piracy, hacking, and either viewing or distributing illegal pornography.

5. Abuse of networks or computers at other sites through the use of the Company's information technology resources will be treated as an abuse of the Company's information technology resources themselves.

6. Computer viruses present a threat to the Company's computing and networking environment. A virus infection may manifest itself in the loss of data, disruption of computer and server software applications, compromises to the security of the network and connected computers, disruption of network services, and lost productivity.

To lessen the threat of computer viruses within the Company's environment, users must be vigilant and avoid any personal use which might expose the Company to the risk of virus infection.

### **Prohibited Activities**

7. As stated above, all users are expected to act in a responsible, ethical, and lawful manner when using the Company's information technology resources. The following are examples, but are not an exhaustive list of prohibited activities.

- a. The use of the Company's information technology resources to attempt unauthorized use or interference with the legitimate use by authorized users of other computers or networks elsewhere which includes misrepresentation of his or her identity to other networks (e.g., IP address "spoofing") from the Company's information technology resources;
- b. Modification or reconfiguration of the software, data, or hardware of the Company's information technology resource (e.g., system/network administration, internal audit) without appropriate authorization or permission;

- c. Knowingly creating, installing, executing, or distributing any malicious code (including but not limited to viruses, worms, and spyware) or another surreptitiously destructive program on any of the Company's information technology resource, regardless of the result;
- d. "Hacking" into other computers or networks;
- e. Copyright infringement including illegal file sharing of video, audio, or data;
- f. Using a computer system attached to the company's resources to capture data packets (e.g., "sniffer") except for authorized or other official company business that includes teaching and learning activities;
- g. Launching denial of service attacks against other users, computer systems, or networks;
- h. Use of the company's information technology resources to transmit abusive, threatening, or harassing material, chain letters, spam, or communications prohibited by law or regulation is prohibited under this policy;
- i. Accessing (e.g., read, write, modify, delete, copy, move) another user's files or electronic mail without the owner's permission regardless of whether the operating system allows this access to occur except in cases where authorized by the company;
- j. Knowingly interfering with the security mechanisms or integrity of the company's information technology resources. Users shall not attempt to circumvent information technology protection schemes or exploit security loopholes;
- k. Connecting devices (switches, routers, hubs, computer systems, and wireless access points as examples) to the network that are not approved by the company. It should be noted that connecting through a company provided authorization process is considered, by default, to be approved access;
- l. Connecting any device that consumes a disproportionate amount of network bandwidth;
- m. Intentionally physically damaging or disabling company computers, networks, or software without authorization.

## **Remediation**

8. Abuse of company policies, resources, or abuse of other sites through the use of information technology resources may result in termination of access,

disciplinary review, termination of employment, legal action, and/or other appropriate disciplinary action.

## **Privacy**

9. The company draws a clear distinction between commercial confidentiality and personal privacy. There should be no expectation of personal privacy in respect of information displayed on, printed using, stored on or sent through company-owned information technology resources and communications infrastructure.

10. The Company reserves the right to preserve and/or inspect any information transmitted through or stored in its computers, including e-mail communications and individual login sessions, without notice.