Information Technology
Acceptable Use Policy

Effective Date: 1 November 2010

The purpose of this policy is to outline the acceptable use of Company's IT resources and to notify employees of the Company’s computer surveillance practices. These policies are in place to protect the employee and the Company.

The individual components of the policy can be expressed in the following terms:

1. To protect Company's networks, equipment and other infrastructure.

2. To reduce the Unsolicited Commercial Email (“Spam")

3. To promote the use of computers and other IT enabled devices to achieve our commercial aims.

4. To protect Company and its employees from activities that might expose either of them to liability.

"Company's resources", means all computer, telecommunications and IT equipment including peripherals (and all other items incidental to computer use) that are owned, used or leased by the Company or its affiliates, the Company's networks, servers and off-site services that the Company subscribes to.

The connection of any device, regardless of ownership or purpose, to any of the Company's resources shall constitute use of the Company's resources. This includes the connection of a device to a mobile (GSM, Wifi, WiMAX, 3G or other mobile network, where the number, service, SIM or bill is paid for or provided by the Company), and the use of such devices shall be governed by this policy.

The policy extends to the use of any Company email account or subscription account provided to the Company by any third party.

While the Company desires to provide a reasonable level of privacy, users should be aware that the data they create on the Company's resources, or while utilizing the Company's resources, is the property of the Company. The Company cannot guarantee the confidentiality of information stored on any computer device belonging to the Company or connected to the Company's resources.

Employees are responsible for exercising good judgment regarding the reasonableness of personal use. The use of the Company’s resources for the carrying on of any business which is not the business of the Company is strictly prohibited. Should use of the Company’s resources for personal purposes or other non-work related purposes be excessive (such determination to be made at the Company’s sole discretion), then the Company may restrict access to the Company’s resources.

The publication (by use of Social Networking/Sharing sites, or otherwise) of details or opinions relating to the policies, procedures or operations of the Company, is prohibited.

For securityand network maintenance purposes, authorised individuals within Company may monitor equipment, systems, individual users and network traffic at any time. The Company may audit networks, systems and individual users for any business purpose. This means that the Company may from time to time monitor your usage of the Company's resources and the content of your work.

Passwords (whether belonging to the Company or a client of the Company) must remain secure and personnel are expressly prohibited from sharing accounts. Authorized users are responsible for the security of their passwords and accounts.

All PCs, laptops and workstations should be secured with a password protected screen saver with the automatic activation feature set at 10 minutes or less (where the machine may expected to be reasonably accessed by a person not authorised to – for example at a sales counter, or a laptop) or 60 minutes or less otherwise, or by logging off or locking the workstation when the system will be unattended.

Company email accounts are provided for business related communications. We permit employees to provide their Company email address to close friends, family and associates provided use of the Company's resources for communicating with such people is kept to a minimum. The use of Company email addresses for all other purposes is prohibited. The use of a Company email account for the carrying on of business other than the business of the Company is strictly prohibited. The company does monitor email communications which pass through the Company's network and may retain such email.

Email accounts provided by a client of the Company are to be used exclusively for the work being performed for that client, and must not be used for personal correspondence or correspondence with the Company.

The surveillance of computer use and of emails which is to be carried out as described above will start on the effective date of this policy and will be ongoing. Such surveillance may be continuous or intermittent.

Any equipment that is connected to the Company's networks must be approved by the Company's IT Manager. Approval will be withheld unless there is an active anti-virus program running on the equipment with current anti-virus definitions. This anti-virus software is available from the Company's IT Manager.

Under no circumstances is an employee authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing the Company's s resources.

The following activities are expressly prohibited:

- Violations of the rights of any person or company protected by privacy laws, copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of

"pirated" or other software products that are not appropriately licensed for use or the duplication or transmission of copyrighted or otherwise protected materials. This provision applies to materials that are considered "Company Confidential."

- The use of any peer-to-peer file sharing software including, but not limited to, BitTorrent, KaZAA, Grokster or Morpheus.
- The use of any IRC or messenger software including, but not limited to AOL or other “Messengers", IRC or "chat" clients (but for the avoidance of doubt, Voice Over IP products are allowed, for business purposes) unless specifically required for work purposes (see below).
- Unless specifically business related, posting or subscribing to blogs, newsgroups, on-line discussion boards or email list groups from the Company's facilities.
- Posting or subscribing to blogs, newsgroups, on-line discussion groups or email lists using a Company email address unless required for reasonable business purposes.
- Participating in any on-line chat unless specifically required for business purposes.
- Revealing your account password to others or allowing use of your account by others. This includes - but is not limited to - family and other household members when work is being done at home.
- Using the Company's resources to engage in activity, or to procure or transmit material, that is in violation of sexual harassment law or any discrimination, vilification, workplace or other law. This includes – but is not limited to – procuring or transmitting pornographic, violent and extremist material.
- Effecting disruptions to, or interfering with, any other computer or network.
- Using any form of network monitoring which will intercept data not specifically intended for the employee unless this activity is a part of the employee's normal job responsibilities.
- Circumventing user authentication or security of any host, network or account.
- Providing information about, or lists of, Company's employees, customers or potential customers to any third party.
- Unauthorized use, or forging, of email header information.
- Connecting to the internet, or sending email through, an anonymous proxy server or similar conveyance designed to obfuscate the user's identity.
- Creating or forwarding "chain letters", "Ponzi" or "pyramid" schemes of any type.
- Installing any software that is not approved by Company's IT Management.
- Copying information to a personal USB memory stick/hard disk/ removable storage player (whether it is a music player or otherwise) except where the devise is approved by the Company’s IT Manager and the copying is only for business purposes.
- The ‘ripping’/copying or storage of music for any purpose.
- The use of third party email accounts for the carrying on of Company business (with the exception of the use of a third party email server to send an email, where the return address is the Company provided email address).

The use of messenger products is allowed when required for business purposes. However, you must register the username and service with messenger@kgpl.com

before using any such service, and have the consent of your manager. In the case of VOIP products, the service that you intend to use, and the unique identifying name that you use must also be registered prior to use with messenger@kgpl.com.

This policy may be changed at any time at the sole discretion of Company. Any changes will be notified to Employees in writing (or by email) and will have full force and effect as if originally incorporated herein. The latest version of the policy is displayed at https://www.kgpl.com/IT/

An employee's breach of this policy shall be grounds for disciplinary action and may result in termination of employment.

The Company's failure to enforce any provision or provisions shall not operate to invalidate Company's rights to enforce any of the provisions of this policy including subsequent changes.

Should any provision of this policy be deemed invalid it shall not effect nor invalidate any other provision.

Note to new employees – if a copy of this policy was not given to you before you commenced employment with the Company then the provisions relating to surveillance of computer usage and emails will not apply to you until 14 days after you first receive notice of or view this policy.