Keltech

Email, Internet and Social Media Policy

1. Policy Statement

Keltech is committed to ensuring email, internet, social media and computer usage that protect the company and its interests while also ensuring dignity at work for all employees.

2. Purpose

The purpose of this policy is to outline the procedure for the use of email, internet, social media and computer resources within Keltech

3. Scope

All employees of Keltech

4. Responsibilities

4.1. Employees are required to familiarise themselves with and adhere to the provisions outlined in this policy.

4.2. Supervisors are responsible for ensuring all employees comply with the terms of this policy.

4.3. The HR Coordinator is responsible for ensuring consistent application of this policy and providing advice and support to supervisors regarding the monitoring and management of this policy.

5. General Principles

5.1. The following list gives examples of conduct that is prohibited in the use of the company’s computer systems. This list should not be considered to be exhaustive.

5.1.1. Violation of copyright laws.

5.1.2. Using the computer or network facilities for unauthorised profit or gain.

5.1.3. Posting, transferring, downloading, viewing or linking to material that is offensive, abusive, threatening or harassing images or material. This includes entertainment software, games images etc.

5.1.4. Unauthorized access to another person’s files or messages.

5.1.5. Use or transfer of unauthorised or unlicensed material.

5.1.6. Personal use of the internet without authorisation.

5.2. Keltech reserves the right and intends to monitor email and internet usage.

5.3. This policy is not exhaustive. In situations that are not expressly governed by this policy, you must ensure that your actions are at all times appropriate and consistent with your responsibilities towards the company.

6. Email

6.1. The email system is to be used solely for the purposes of Keltech and not for personal purposes of employees. Personal emails should only be sent in exceptional circumstances.

6.2. E-mails should be regarded as potentially public information which carry a heightened risk of liability for the sender, the recipient and the company.

6.3. An e-mail should be regarded as written formal correspondence, the recipients of which may be much wider than the sender intended, hence any defamatory or inappropriate remarks have serious consequences as can any indirect innuendo.

6.4. E-mail has the same permanence and legal status as hard copy. Employees must ensure that the same professional standards that apply to other written documentation are also applied to e-mails, including levels of confidentiality. E-mails to outside organisations have the same power to create binding contracts as hard copy documents.

6.5. When communicating using e-mail it is important for employees to be respectful and clear as if you were writing a formal business letter. Each mail sent should identify the subject matter. If the mail is private it should be identified as such.

6.6. Particular care should be taken when sending confidential or sensitive information internally or to parties outside of the company. Please ensure to password protect any confidential or sensitive attachments.

6.7. Users must not send messages, including attachments, which are abusive, threatening, defamatory, offensive, harassing, obscene, racist, sexist or other inappropriate remarks whether in written, cartoon form or otherwise.

6.8. Users must not partake in or promote the sending or distribution of chain email messages or send unnecessary files which would adversely affect computer and network resources.

6.9. If an employee receives any offensive, unpleasant, harassing or intimidating messages via e-mail they should contact their supervisor immediately.

6.10. E-mail messages/attachments can carry computer viruses which are particularly harmful to the company computer systems. Hence, it is critical that the Purchasing Manager is contacted if an employee receives an e-mail from an unknown sender or an e-mail which may contain a virus. Under no circumstances should an employee respond to spam emails.

7. Internet

7.1. Access to the internet is solely for business purposes during working hours. Access during breaks is permitted and use outside of working hours is allowed with the agreement of your supervisor. Where permission is granted usage must at all times be in line with the terms of this policy.

7.2. There is no quality control process on the internet and a considerable amount of information published on the internet is outdated, inaccurate or deliberately misleading. All information obtained from the internet should be considered with caution until confirmed by a reliable source.

7.3. Employees must at all times respect copyright and intellectual property rights of information which they encounter on the internet. Proper credit to the source of information used for company purposes must be given.

7.4. Internet access may potentially provide employees with access to material unsuitable for the work place. It is strictly against Company policy for employees to download, view, send and knowingly receive any material that may potentially be considered:

7.4.1. Offensive (for example: discriminatory on the grounds of sex, age, religion, race, colour, sexual orientation, ethnic or national origin or disability. This includes jokes, text, pictures, or such materials that have the potential to cause offence)

7.4.2. Intimidatory (for example: threatening text or picture)

7.4.3. To leave Keltech open to criminal or civil action (for example: potentially illegal information, libellous material, breach of copyright law and material likely to cause offence).

8. Social Media

8.1. Social media refers to the use of web based and mobile applications for social interaction and the exchange of user-generated content. Social media channels include Facebook, Twitter, Linkedln, You Tube, Flickr, Blogs, review sites, forums and any similar online platforms.

8.2. Keltech is committed to utilising social media to enhance its profile and reputation, to listen and respond to customer opinions and feedback, and drive revenue, loyalty and advocacy. We encourage employees to support our activities through their personal social networking channels while adhering to the guidelines outlined in this policy.

8.3. Employees are encouraged to become fans and followers of the company's profile and to share company generated content within their personal networks. However, the company's channels are administered by designated people only and all official content must be approved and distributed by them.

8.4. Access to social media sites for personal purposes is not permitted during working hours. Access during breaks is permitted and use outside of working hours is allowed with the agreement of your supervisor. Where permission is granted usage must at all times be in line with the terms of this policy.

8.5. When using social media sites employees should always be mindful of what they are posting, who can see it, and how it can be linked back to the company and work colleagues. Behaviour and content that may be deemed disrespectful, dishonest, offensive, harassing or damaging to the company's interests or reputation are not permitted. Employees must not disclose private and confidential information about the company, its employees, clients, suppliers or customers on social networks.

8.6. Keltech reserves the right to utilise for disciplinary purposes any information that could have a negative effect on the company or its employees, which management comes across in regular internet monitoring, or is brought to their attention by employees, customers, members of the public etc.

9. Anti-Virus and Data Protection

9.1. An employee who suspects a PC / laptop has been infected with a virus must notify their supervisor immediately.

9.2. Kel-Tech Engineering network antivirus system and spam arrest are regularly monitored.

9.3. All data stored on the Company's equipment is the property of Kel–Tech Engineering Ltd.

9.4. Employees should not omit to do anything which may lead to any information held on IT Systems to be lost, disclosed or accessed by third parties.

9.5. Maintaining password privacy is the responsibility of each individual employee and consequently employees are responsible for any abuses taking place using their name and password.

9.6. All critical data on laptops or local hard drives must be backed up onto the Network or a removable device on a regular basis. This is the responsibility of the user.

10. Computer Equipment

10.1. Computer equipment must be treated with care. Any damage must be reported to your supervisor or the Purchasing Manager.

10.2. In order to maximise the efficiency of the computer network and minimise the risk of viruses, PCs may only be loaded with Company approved software in conjunction with the Purchasing Manager.

10.3. All documents / files copied to external devices (USB storage/disks) are covered by the general confidentiality obligations which apply to all aspects of your employment.

10.4. All PCs / laptops will be scanned periodically to complete a hardware and software audit.

10.5. Uploading of non licensed software (i.e. pirate copies) to any of Kel-Tech Engineering's computer equipment is strictly prohibited. If you are in any doubt you should contact the Facility/ Utility Manager.

10.6. Any unauthorised software that has been installed will be removed.

10.7. Non–employees of Kel–Tech Engineering, including partners and children are not permitted to use the Company's equipment without prior permission.

10.8. Company laptops should not be left in unattended vehicles.

10.9. Company laptops should be kept as hand luggage when travelling.

10.10. Any act or misuse of computer equipment may be found as misconduct and may lead to disciplinary procedure.

11. Locking Unattended Computer Screens

11.1. Desktop computers and other devices logged into Keltech computer accounts must not be left unlocked and unattended in a way that risks access by an unauthorised user.

11.2. It is therefore essential that the habit of routinely locking unattended screens is widely established. This may also be additionally by additionally secured screensavers to automatically lock and apply password protection after a time of inactivity.

12. Breach of the Policy

Any breach of this policy may lead to disciplinary action up to and including dismissal.