IT, Internet & Social Networking Use Policy

Please read all pages of this document carefully and then sign below.
(All Company employees, contractors or temporary staff who have been granted the right to use the Company's Internet access are required to sign this agreement confirming their understanding and acceptance of this policy.

Location: ……..…….

Employee Name: ……..…….

Employee Signature: ……..…….

Date: ……

IT Policy

Due to recent technological changes introduced to protect ICTS (UK) Ltd's ("ICTS") systems you should be aware that ICTS has the ability to monitor outgoing Internet connections on any ICTS IT equipment or system. ICTS reserves the right to monitor the internet usage of any employee at any time during their employment with the company.

ICTS provides you with access to a variety of information technology systems and electronic communication media for the execution of your duties to support the operation of the ICTS business. All electronic communication systems and all communications and stored information sent, reserved, created on or contained within these systems belong to ICTS.

ICTS has access to, and reserves the right to retrieve and review, information on its IT systems including information that you have protected by password.

ICTS' communications systems must not be used for conveying inappropriate messages that may be considered defamatory, derogatory, obscene, offensive or discriminatory. You will be potentially liable for legal claims arising from the sending of inappropriate material internally or externally. Employees may be subject to disciplinary action and contractors will be dealt with accordingly.

You are responsible for maintaining the confidentiality of all material contained on all systems for which you have responsibility. It is vital that you password protect your PC or laptop. Any discovery of a lapse in IT security must be reported as a matter of urgency to the IT Department. Passwords for access to the system are confidential and must not be revealed to other persons, unless you are specifically requested to do so by the IT department.

You are prohibited from removing from ICTS' premises any hardware, software, files or data without express written permission from the IT Manager. Equally, you are prohibited from adding any personal hardware, software, files or data without express written permission from the IT Manager. Creation of files and data must only be done so within the execution of your duties, and the creation of any other data is prohibited.

ICTS' software and data must not be copied or transmitted to any hardware, internet site, or network not owned, leased or controlled by ICTS e.g. using personal devices to access email or Office 365 is strictly prohibited. The use of removable storage media (including USB flash drives) are prohibited unless expressly authorised by the IT Manager.

No employee may use an access code or password to access a file or retrieve any stored communication in any other employee's area of ICTS' systems unless authorised to do so by IT.

Staff have free access through their workstations. No other equipment shall be connected to the Internet via a telephone or network connection unless approved by the IT Department, nor shall any unauthorised software be downloaded or installed on ICTS IT equipment.

No equipment that could permit access to the Internet, or allow anyone to connect by any means, I.E. via a wireless connection, is to be connected to the ICTS' network or hardware. No alterations to the set-up of any ICTS IT equipment may be made without the prior written approval of the IT Department.

Upon the discovery, or suspicion, of computer virus the IT Department must be advised immediately.

Any mobile company device with Outlook, Office 365 or One drive must be password/pin protected. In addition they must not have personal accounts connected to the mobile device.

Staff must ensure that no visitor to the office connects any equipment that would allow ICTS Internet access without the permission of the IT Department.

The creation, generation, and distribution of materials that are offensive on the grounds of any protected characteristic, perceived or actual, are forbidden and will be considered to be gross misconduct.
The protected characteristics are:-

- Age
- Disability
- Gender Reassignment
- Marriage and Civil Partnership
- Pregnancy and Maternity
- Race (including colour, nationality, ethnic or national origin)
- Religion or Belief
- Sex
- Sexual Orientation

It is forbidden to use the computer system to generate and/or distribute material which is offensive to or ridicules other employees.

The storage of any kind of offensive material (including pornography) on the computer system is expressly forbidden.

In respect of these rules material will be considered offensive if it causes distress to the person who receives or discovers it.

Failure to adhere to the terms of the above policy may result in disciplinary action, up to and including dismissal, being taken against you.

Internet Use Policy

Use of the Internet by employees of ICTS (UK) Ltd. ("ICTS") is permitted and encouraged where such use supports ICTS' goals and business objectives. Occasional, limited personal use of the Internet is acceptable subject to its compliance with ICTS' Internet Policy.

ICTS' policy for the use of the Internet requires that employees:

1) Comply with all current legislation;
2) Use the Internet in a manner acceptable to ICTS;
3) Do not create any business risk to ICTS by their use of the Internet – or in any way whatsoever;
4) Do not do or cause to be done anything that may compromise ICTS' reputation or business;
5) Maintain the confidentiality of ICTS' business information when using the Internet
6) Behave in a generally responsible fashion when using the internet

All employees are responsible for ensuring that their Internet use is within these regulations and is both ethical and lawful.

Please note that this list is not exhaustive.

A. Responsibilities of Internet Users

ICTS prohibits the following use of the Internet by its employees:

1) The downloading of text or images which contain material of an offensive, indecent or obscene nature.

2) The transmission of any message in which the origin is deliberately misleading. If a user transmits, or causes to be transmitted, a message that is inconsistent with ICTS' business goals or with a misleading origin, the person who performed the transmission will be solely accountable for the message and not ICTS which is solely acting as the information carrier.
3) Using ICTS' IT systems to perpetrate any form of fraud or software piracy.

4) Using the Internet to send offensive or harassing material to other users, either internally or externally

5) Accessing or retrieving any information via the internal network, or the Internet if they do not have full legal, authorised access to the information.

6) Creating or transmitting defamatory material.

7) Undertaking deliberate activities that waste staff effort or networked resources. Introducing any form of computer virus into the corporate network.

8) ICTS employees must not, without prior approval from the IT Manager (or appropriate deputy), utilise, for example, any of the following technologies: peer-to-peer (P2P), E.G. Bittorrent, Emule, VPN, routing, forwarding, on any computer connected to the ICTS data network for the purposes of sending data to or receiving data from an externally located machine.

This list is not exhaustive and the company reserves the right to make amendments where we deem it to be appropriate. Any amendments to the contents of this policy may be without notice and therefore, it is your responsibility to ensure that you are fully conversant with the content of this policy at all times.

B. Email Code of conduct

This section sets out our e-mail code of conduct so that any employee who:-

1) Uses e-mail technology on our behalf;

2) Uses the technology on hardware, software we provide;

3) Uses the technology to communicate information about us, our customers and/or suppliers;

4) Uses the technology to communicate any information that has been gained from us.

The employee does so in accordance with this code of conduct.

Caution must be taken when using e-mail as it is easy to send. **BUT** once the send command has been given, the message cannot be stopped. E-mail can create binding contracts.

It is forbidden to:-

- access or distribute pornography;
- take part in electronic chain letters;
- post confidential information about us, our customers or suppliers without authorisation;
- send junk e-mail;
- bully, harass or abuse others through the use of e-mail. This includes sending information that insults or harasses others with respect to their sex, race, age, disability or religion, or any other characteristic; perceived or actual
- download, open or distribute unauthorised or copyrighted material or software;
- post confidential information about us, our customers or suppliers without authorisation;

When replying to an e-mail, make sure that the reply is for the sender only and not original mailing list (unless there is a requirement to do so).

When attaching files to a message, keep them small. In addition, do not attach files that have hidden confidential information (e.g. base cost calculations you may have used to generate a quote). Software exists that can reveal this hidden data.

Make sure that the content of your e-mail is factually correct and non-defamatory.

If you receive an electronic communication from within ICTS which contains content which you consider to be offensive, it is your responsibility to report the matter to the IT Manager immediately.

Should you be subject to harassment or abuse from e-mail at work from another employee, then the matter should be reported through the Grievance Procedure immediately.

D. Virus warning emails, scam warnings email, chain emails and hoax emails.

Such emails are relatively common, and can often be of little or no merit. If you receive an email warning you of a virus etc, ICTS (UK) Ltd systems should not be utilised to help propagate it. Contact the ICTS (UK) Ltd IT Department and if requested send them a copy of the email. Do not forward to any other party than the IT Department, who will assess the validity of the warning and take any further appropriate action.

You must not send or forward this type of mail to anyone; internally or externally. Doing so internally creates unnecessary email, and sending this type of email to clients and/or other external third parties may reflect poorly on the Company.

E. Downloading

Any software or files downloaded via the Internet onto ICTS equipment may be used only in ways that are consistent with their licences or copyrights.

No user may use ICTS facilities to download or distribute illegal software or material.

No user may use the ICTS Internet facilities to propagate any virus, spyware, malware, or other software that the Company considers may be of detriment to an end user.

F. Chat, blogs, newsgroups and Social Media sites

Chats, blogs, newsgroups and social networking sites are public forums. Information placed on these websites is public, not secure and may appear in unexpected places. Improper use may pose a risk to the Company's security and reputation and, in order to safeguard both, the following rules apply, regardless of whether or not this is within an employee's working hours, or using systems which belong to the company;

1). Confidential ICTS or personal information **must not** be revealed and any comments or photographs which are defamatory to the company, its business or its clients, are not to be posted by employees.

2). Employees may participate in newsgroups, blogs, or chats in the course of their work, but they do so as individuals, speaking only for themselves. Only those users who are duly authorised to speak to the media on behalf of ICTS may write in the name of the Company to any newsgroup or Web site.

3). ICTS retains the copyright to any material posted to any forum, newsgroup, chat, blog or World Wide Web page by any employee in the course of his or her duties.

4). Material posted using social media should not disclose Company work-related information, especially confidential or privileged data, even when posted in your own time or using your personal internet access.

5). Employees are ambassadors for the company and should exercise care and restraint if mentioning the company online. Improper or unauthorised use of the Company name, or discussing sensitive or inappropriate workplace issues, which may bring you, your colleagues, the Company or its clients or suppliers into disrepute, is not acceptable and may lead to disciplinary action, up to and including dismissal.

6). The lines between public and private, personal and professional lives are blurred in online networks. If you publish to a social media site and in doing so mention the Company, its employees, clients or suppliers, or if you or the posted material can be identified as being related to the Company, its employees, clients or suppliers in any way, you must make it clear that the views and opinions you express are your own, and not those of the company.

7). You must not publish unauthorised user generated content, e.g. video footage or photographs of Company facilities, staff, or projects relating to our clients.

8). If you come across any online material that is potentially damaging to the Company's reputation, you should report it immediately to the HR Manager.

9). Should you wish to set up a social networking site/blog bearing the Company's name and/or logo, e.g. for recruitment or professional purposes, you must first obtain the express approval of your line manager and Corporate Communications. Failure to do so will be considered to be a fundamental breach of this policy. Any such site should adhere to these guidelines and be kept up to date.

Auditing

ICTS accepts that the use of the Internet is a valuable business tool. However, misuse of this facility can have a negative impact upon employee productivity and the reputation of the business.

In addition, all of the company's Internet-related resources are provided for business purposes. Therefore, the company maintains the right to monitor the volume of Internet and network traffic, together with the Internet sites visited. *The specific content of any transactions will not be monitored unless there is a suspicion of improper use.* Users should not have any expectation of privacy as to his or her Internet usage.

ICTS may provide you with access to a variety of information technology systems and electronic communication media for the operation of our business. All electronic communication systems and all communications and stored information sent, reserved, created on or contained within ICTS' equipment are ICTS' property.

ICTS has access to, and reserves the right to retrieve and review, information on any of its IT systems, including information that you have protected by password.

Non Compliance

Failure to comply with the contents of this policy may result in disciplinary action being taken against you. Misuse of ICTS' computers or unauthorised access to the computers or misuse of email, Internet or Company information will be viewed as a potential Gross Misconduct matter.
The company views compliance with the IT policy and sub policies contained within as being of the utmost importance. Any breach of this policy will be addressed in accordance with the company's disciplinary procedure, which may, in turn, result in the summary termination of your employment.

Social Networking Policy

You should not make contributions relating to this organisation on social networking sites unless part of your role. You should not comment about any other employee, client, supplier etc. This applies whether you use our equipment or your own and whether in work time or your own. Such contributions may impact detrimentally upon our interests, whether inadvertently or otherwise. We will view infringements as a serious breach of our rules. This may result in disciplinary action and, potentially, dismissal.

We hold you accountable for all contributions that you make or that are posted under your user name or account details. Anything you post can impact upon us even if you did not intend this. It does not matter whether your post was made personally or on your behalf. Consider carefully whether what you intend to say could be detrimental to our interests. You should take great care not to post anything that could be considered inflammatory. You must ensure you do not publish inaccurate, inappropriate or defamatory content. We will view infringements as a serious breach of our rules. This may result in disciplinary action and, potentially, dismissal.

We appreciate that many people use social networking sites such as LinkedIn or Twitter. You may do this personally or even in your professional capacity on our behalf. If you identify details of your role within our organisation, we can clearly be associated with what you say. Therefore, anything you post on such sites must not infringe the provisions above.

You may also develop a database of contacts on such sites. It will inevitably contain a mixture of connections. You may obtain some from our contact database. You may create some with our clients, other employees etc. during your employment. Some may be contacts from former roles or your personal acquaintances. Where you develop contacts through your work on our behalf, our confidentiality provisions apply. You must respect them even after you leave our employment. Confidential information includes, but is not limited to, information and data about other employees, customers, clients, suppliers etc. We may require you to supply details of contacts established as part of your employment before you leave. We may require you to delete such contacts from your account(s) at our entire discretion.

Where you have a grievance or concern about something associated with work, do not use social networking to air it. You should normally discuss it with your line manager at an early opportunity. We also have a confidential reporting system which is available to all employees. This provides you with an appropriate means of raising matters of concern about any aspect of our organisation.

The above rules apply also to professional networking sites, such as LinkedIn. There is a public affiliation between user and employer and employees are reminded of the company's rules with regards to statements to the media, which state that only the Managing Director is authorised to make any communication or statement to the media, or delegate this responsibility to another person, in matters relating to the business. Failure to comply with this may result in disciplinary action up to and including dismissal