Pell Frischmann

ACCEPTABLE USE AND MONITORING POLICY: COMPUTING, SOFTWARE, INTERNET and EMAIL

The Company's policy on the acceptable use and monitoring of computing, software, Internet and email applies to all companies in the Pell Frischmann Consulting Engineers Ltd Group including any subsidiaries.

This Acceptable Use and Monitoring Policy applies to all staff of the Company and to those who are offered access to the Company's computing and telecommunication resources ("the Facilities").

This Policy is reviewed regularly and applies to all staff, including mobile computer users, and those users who may be working remotely from the office with company owned facilities.

It is the responsibility of all staff to read, fully understand and sign agreement to the Acceptable Use and Monitoring Policy.

Iain Bisset

Iain Bisset
Managing Director
1 March 2020

1. GENERAL PRINCIPLES

Use of computing facilities, software, the Internet and Email is encouraged for professional use, where such use is for business purposes and supports the goals and objectives of the Company. All Facilities are to be used in a manner that is consistent with the Company's standards of business conduct and as part of the normal execution of an employee's professional job responsibilities.

- The Company's Acceptable Use Policy is implemented to safeguard the Company from prosecution under numerous laws surrounding the use of computers, software, Internet and Email.
- Use of the Facilities, Software Applications, the Internet and Email will be subject to monitoring for security and/or network management reasons. Users may also be subject to limitations on their use of such resources if such use has been abused by the user.
- Email accounts, Internet Ids and web pages should not be used for any unauthorised or illegal communications.
- The distribution of any information through the Internet, computer-based services, Email, and messaging systems is subject to scrutiny by the Company; and the Company reserves the right to determine the suitability of this information.
- The use of computing resources is subject to the appropriate laws and any illegal use will be dealt with appropriately.
- The use of the Computing Facilities, Email, Internet and software is solely to conduct Company business. The Company treats all information transmitted through or stored on any of their systems, including Email messages as Company business information. All Email messages are and remain the property of the Company. They are not the private property of any employee.

2. COMPUTING FACILITIES

- All computing equipment required by the Company must be purchased by IT Services. No other staff may purchase computing equipment without the express permission in writing of IT Services, e.g. the purchase of computing equipment by any other means such as credit cards, expense accounts or petty cash is expressly forbidden.
- All newly purchased computing equipment will be delivered directly to IT Services, wherever possible so that it can be checked and Asset Registers updated. No other staff may unpack newly delivered computing equipment.
- Computing equipment can only be installed by IT Services. Under no circumstances is computer equipment to be installed by any other member of staff unless express permission has been given in writing.

Users Shall Not:

- Move (or attempt to move) fixed computing equipment without informing and gaining approval in writing from IT Services; including desktop computers and printers.
- Tamper with, "open up" or upgrade any computing equipment. Under no circumstances is computer equipment to be upgraded by any other member of staff unless express permission has been obtained in writing.
- Disposal of computing equipment may only be carried out by IT Services.

3. SOFTWARE APPLICATIONS

It is the policy of the Company to respect all computer software copyrights and adhere to the Terms & Conditions of any licence to which the Company is a party.

The Company will not condone the use of any software that does not have a legal licence.

- All computer software required by the Company must be purchased by IT Services. No other staff may purchase software without the express permission in writing from the

Company, and the purchase of software by any other means such as credit cards, expense accounts or petty cash is expressly forbidden.

- All newly purchased software will be delivered directly to IT Services so that licences can be checked and Asset Registers updated. No other staff may take delivery of computer software unless express permission has been given by IT Services in advance.
- Computer Software can only be installed by IT Services regardless of source. Under no circumstances is computer software to be installed by any other member of staff unless express permission has been given in advance by IT Services.
- The use of mobile computing solutions is becoming more prevalent and the ability to synchronise hardware with business systems heightens the Company's exposure to viruses, unlicensed software, pornography and other copyrighted material and as such is prohibited unless express permission has been given by the Company.

Users Shall Not:

- Copy or move (or attempt to copy or move) any software.
- Dispose of any software or software licenses which have been used by the Company. Disposal of software may only be carried out by IT Services.
- Install (or attempt to install) games, screensavers, shareware, freeware or public domain software.
- Install (or attempt to install) any software supplied by a contractor, client or other third party (regardless of source) unless express permission has been given in writing by the Company.

4. INTERNET

Users Shall Not:

- Use any other system than that explicitly authorised by the Company for the Internet.
- Visit Internet sites for non-related business activity, e.g. any Internet sites that may contain obscene, hateful or other objectionable materials. Control mechanisms will be adopted by the Company to implement specific URL filtering and compliance to the Platform for Internet Content Selection (PICS), including the SafeSurf Ratings.
- Make or post indecent and/or offensive remarks, proposals, or materials on the Internet. Among those that are considered to be offensive are any messages which contain sexual implications, racial slurs, gender specific comments, or any other comments that offensively address someone's gender, marital status, age, sexual orientation, religion or belief, race, nationality or ethnic origin or disability. Employees should not post any information on the Internet, eg on blogging sites that may be considered detrimental in any way to the Company or towards an individual or group of individuals.
- Download (or attempt to download) any software or applications without the express permission in writing from the Company.
- Install (or attempt to install) any downloaded software supplied by a contractor, client or other third party (regardless of source) unless express permission has been given in writing by IT Services

5. EMAIL

- Email is a formal means of communication and must be used in a professional manner. Users should note that:
  - Emails can be used as evidence in a court of law.
  - Email is immediate; please remember this when constructing your Emails.
  - Email is not a secure means of communication and is not confidential.
  - Offers and contracts made by Email can be considered legally binding.
  - Jokes, sarcasm, tone and content of Emails can be easily misinterpreted.
- Always use care in addressing Email messages to make sure that the messages are not inadvertently sent to the wrong person. Exercise care when using distribution lists and take measures to ensure that the lists are current.

- Your Email messages may be read by someone other than the person to whom you send them. Someday they may have to be disclosed to outside parties or a court in connection with litigation. Accordingly, your Email messages should be courteous, professional and businesslike.

Attorney-client Privileged Communication

Some Email messages may constitute confidential privileged communications between the Company and its attorneys. Do not forward messages from counsel to any other party without counsel's approval. Do not send copies of messages to counsel to other employees who are not involved with the subject of the message without counsel's approval.

Users Shall Not:

- Use any other system than that explicitly authorised by the Company for Email.
- Send or solicit Emails that are unrelated to business activities or for personal gain. As with the Company telephone system, limited use of the Company Email system will be allowed for personal Emails, provided the system is not abused and is used in accordance with the existing controls and procedures.
- Send or solicit Emails that are obscene, defamatory or intended to annoy, harass or intimidate another person.
- Use the Email system to disseminate off-coloured jokes, promote chain letters, or other similar types of activities.
- Make defamatory, racial or sexual remarks about of the Company.
- Install (or attempt to install) any software supplied by a contractor, client or other third party (regardless of source) unless express permission has been given in writing by the Company.
- Attack the security or privacy of other individuals or organisations.
- Carry out 'Spamming' or 'mass mailing' to external individuals or organisations.

6. CONFIDENTIALITY

Everyone must exercise caution in transmitting confidential Company information because of the reduced effort required in electronic communication. Confidential Company information should never be transmitted or forwarded to outside individuals or companies that are not authorised to receive the information. Confidential information should not be sent to other employees inside the Company who do not need to know the information.

Users Shall Not:

- Upload, download, or otherwise transmit software belonging to parties outside the Company, or the Company itself, without the permission of IT Services.
- Upload, download, or otherwise transmit any other copyrighted materials to parties outside the Company, or the Company itself, without written consent from the Company.
- Illegally or unprofessionally reveal or publicise confidential or proprietary information which includes, but is not limited to: financial information, new business and product ideas, marketing strategies and plans, databases and the information contained therein, client lists, technical product information, computer software source codes, computer/network access codes, and business relationships.

7. SECURITY

- Access to the Company's system is controlled through the use of usernames and passwords. Once you have agreed to abide by the Company's Acceptable Use and Monitoring Policy, you will be issued with a username and password. Passwords are alphanumeric; at least 8 characters long, must contain at least 3 different character types (i.e. Uppercase, Lowercase, Number or Special Character such as ! % ~ # > < + = - : ; " '), must not be a password that you have used previously and must not contain your username. You will be prompted to change your password every 35 days. You must not share your password and whilst logged on to the computer network you will be responsible for all transactions. You will be expected to 'log-out' when not using the computer for any length of time (especially at night). If you need to work on a PC other than that allocated to you, you need to log on to that PC using own username and password.
- It is an offence under the Computer Misuse Act, 1990 Section C, to access (or attempt to access) computer held data, or software, without the authority to do so.
- All data relating to living individuals must be registered and processed in accordance with the Company's Data Protection registration. Processing of such data may only be made on computers owned by the Company and physically located within Company premises or securely connected remotely to the Company by IT Services.

Users Shall Not:

- Intentionally interfere with the normal operation of the network; including the propagation of computer viruses, spy-ware, ad-ware and sustained high volume network traffic that could hinder others in their use of the network and could increase the possibility of a security attack.
- Interfere with the Anti-Virus software and/or other back-office applications which monitor and safeguard the Company's systems.
- Short-circuit the working procedures and instructions that relate to the security and confidentiality of the network, and the data stored across the network.
- Document or divulge passwords to parties outside the Company, or to non IT staff within the Company itself without express permission.
- Examine or change access permissions for which they do not have explicit authorisation from IT Services.
- Use another person's user name, files, or output for which they do not have explicit authorisation.
- If any user believes that they have privileges or access to software, data or systems which they should not have, this should be reported to IT Services immediately.

8. WORKING REMOTELY FROM THE OFFICE WITH COMPANY FACILITIES

It is the employees' responsibility to ensure that:

- Company owned facilities are used for business purposes only. Personal and recreational use (including outside business interests) is not permitted.
- Company owned facilities and the Company network are not used by family members. Any activities that violate the Company's policies will be the responsibility of the employee.
- Company owned facilities are not re-configured by anyone other than a member of IT Services.
- Personal equipment is not used to connect to the Company computer network.

The following points should be noted:

- Remote access to the Company's corporate computer network will be controlled and access is provided only with Company owned facilities.

- All Company owned Facilities will be configured and supported by IT Services, and will use standard approved configurations to minimize resource requirements.
- Remote access is provided and supported by the Company on the basis of 'best endeavours'. The Company has not provisioned additional resource for remote access services, nor does the Company provide support outside normal business hours.
- If for any reason there is a problem with the remote service, it is the responsibility of the employee to make alternative arrangements and work from a company office.
- At no time should any company employee provide their username and password to anyone, not even family members.

9. MONITORING

The following points are noted, as these are in line with new Employment Law. At the current time the Company does not carry out all of these principles, but it reserves the right so to do:

- The Company may monitor the use of any of its computer systems, including the Internet and Email. Accordingly, employees should not use the system to send, store, or receive any personal information they wish to keep secret. Any such information, if found, will be removed.
- The Company recognises the importance of an individual's privacy but needs to balance this against the requirement to protect others and to ensure that the facilities are not misused.
- The principal reasons for monitoring the Facilities are to:
  - Detect any harassment or similar misconduct by employees and to ensure that the Company complies with its legal obligations. These legal obligations include those contained in contracts of employment and in relevant policies, including health and safety, disciplinary and equal opportunities.
  - Ensure compliance with this Policy.
  - Ensure the integrity of the Facilities and any sensitive or confidential information belonging to the Company.
  - Ensure compliance by users of the Facilities with all applicable laws (including Data Protection), regulations and guidelines published and in force from time to time.
- The Company may adopt at any time a number of methods to monitor use of the Facilities. These may include:
  - Recording, auditing and logging of internal, inter-office and external telephone calls made or received by employees using its telephone network (including where possible mobile telephones). Such recording may include details of length, date and content.
  - Recording, auditing and logging the activities by individual users of the Facilities. This may include opening Emails and their attachments, monitoring Internet usage including time spent on the Internet and web sites visited.
  - Record and log access to restricted or controlled areas of the business. Such recording may include CCTV, details of length, date and content.
  - Physical inspections and audits of an individual users computer, software and telephone messaging services.
  - Monitoring of the Facilities through third party software including real time inspections.
  - Physical inspection of an individual's post.
  - Archiving of any information obtained from the above including Emails, telephone call logs and Internet downloads.
- If an employee wishes to use the Facilities for private purposes without the possibility of such use being monitored, they should contact the Company in writing. The Company will then consider the request and any restrictions upon which such consent is to be given. In the event that such request is granted the Company (unless required by law) will not monitor the applicable private use.

- The Company will not (unless required by law):
  - Allow third parties to monitor the Facilities; or
  - Disclose information obtained by such monitoring of the Facilities to third parties.
- The Company may be prohibited by law from notifying employees using the Facilities of a disclosure to third parties.

All employees are required to adhere to the instructions contained within this policy. Failure to do so may result in a disciplinary process that may lead to dismissal. The Company also reserves the right to report any illegal violations to the appropriate authorities.