POLICY NAME	**E-Mail, Computer Network & Internet Access Policy**
PURPOSE	**To provide clear rules and guidelines for the Company and its employees on the acceptable use of the Company's computer network, internet access and email usage.**
APPLIES TO	**All Staff**
DATE IMPLEMENTED	**January 2015**

1 Introduction

1.1 In this Policy Arctics Ltd (trading as Igloo) is referred to as the 'Company'. For the avoidance of doubt these rules and procedures should be followed at all times at your individual location of work. In the event that you are placed at a clients' premises you should adhere to their own policies and procedures where they differ to the rules and procedures set out by Igloo.

1.2 Users accessing the internet do so at their own risk and the Company cannot be held responsible for material viewed or downloaded by users. To minimise these risks, your use of the internet during your employment is governed by the following policy.

2 Permitted use of the Internet and Computer Network

2.1 Legitimate Business Use

2.1.1 The computer network is the property of the Company and should be used primarily for legitimate business purposes. Users are provided access to the computer network to assist them in the performance of their jobs. Additionally, certain employees have been provided with access to the Internet through the computer network. All users have a responsibility to use the Company's computer resources and the internet in a professional, lawful and ethical manner. Abuse of the computer network or the internet may result in disciplinary action, including possible termination, and civil and/or criminal liability.

2.2 Passwords

2.2.1 Users may be issued with a password for some or all of the parts of the computer network which they may access. Users are responsible for the security of their passwords. If they suspect their security has been breached then this should be reported to their direct Manager immediately.

2.3 Personal Use

2.3.1 Employees are authorised to use the internet for personal purposes before or after work and during their lunch break only; however access to inappropriate websites is still prohibited.

2.4 Prohibited Uses

2.4.1 Without prior permission from the Company, the Company computer network may not be used to disseminate, view or store commercial or personal advertisements, solicitations, promotions, destructive code (e.g. viruses, self-replicating programs etc), political material, pornographic text or images, or any other unauthorised materials.

2.4.2 Employees may not use the Company's Internet connection to stream, download games or other entertainment software.

2.4.3 Employees may not use the computer network to display, store or send (by e-mail or any other form of electronic communication such as bulletin boards, chat rooms, user net groups etc.) material that is fraudulent, harassing, embarrassing, sexually explicit, profane, obscene, intimidating, defamatory, discriminatory or otherwise inappropriate or unlawful. Furthermore, anyone receiving such material should notify their direct Manager immediately.

2.5 Illegal Copying

2.5.1 Users may not illegally copy material protected under copyright law or make that material available to others for copying. Employees are responsible for complying with copyright law and applicable licenses that may apply to software, files, graphics, documents, messages, and other material that they wish to download or copy. No employee may agree to a licence or download any material for which a registration fee is charged without first obtaining the express written permission of the Company.

3 Duty not to Waste or Damage Computer Resources

3.1 Virus Protection

3.1.1 In order to prevent the introduction of virus contamination into the software system, the following must be observed:

- Unauthorised software including public domain software, magazine cover disks/CDs or Internet/World Wide Web downloads must not be used;
- All software must be virus checked using standard testing procedures (contact your immediate Manager for details) before being used.

3.1.2 Files obtained from sources outside the Company (including discs from home, downloaded from e-mail or the internet) may contain dangerous viruses that may damage the Company's computer network. If you suspect that a virus has been introduced into the Company's network, you must notify the Company immediately. It is a disciplinary offence to deliberately import a virus into the Company's computer network.

3.2 Frivolous Use

3.2.1 Computer resources are not unlimited. Network bandwidth and storage capacity have finite limits and all users connected to the network have a responsibility to conserve these resources. As such, the user must not deliberately perform acts that waste computer resources or unfairly monopolise resources to the exclusion of others. These acts include, but are not limited to, sending mass mailings or chain letters, spending excessive

amounts of time on the Internet, playing games, engaging in online chat groups, uploading or downloading large files, accessing streaming audio and/or video files, or otherwise creating unnecessary loads on network traffic associated with non-business-related uses of the Internet.

3.3 No Expectation of Privacy

3.3.1 Employees are given computers and Internet access to assist them in the performance of their jobs. Employees should have no expectation of privacy in anything they create, store, send or receive using the Company's computer equipment. The computer network is the property of the Company and may be used only for Company purposes.

3.4 Waiver or privacy rights

3.4.1 Users expressly waive any right of privacy in anything they create, store, send or receive using the Company's computer equipment or internet access. Users consent to allow Company personnel access to and review of all materials created, stored, sent or received by users through any Company network or Internet connection.

3.5 Monitoring

3.5.1 The Company has the right to monitor and log all aspects of its computer system including, but not limited to, monitoring internet sites visited by users, monitoring chat and newsgroups, monitoring file downloads and all communications both sent and received by users.

3.6 Blocking sites with inappropriate content

3.6.1 The Company has the right to utilise software that makes it possible to identify and block access to Internet sites containing sexually explicit or other material deemed inappropriate in the workplace.

4 E-mail Use

4.1 It should be noted that no guarantees can be given with regard to the privacy of any e-mail system and this includes the Company's.

4.2 Employees may not use the computer to send email correspondence to friends or family.

4.3 Employees must not waste time or congest the system by sending trivial messages, mass mailings, unnecessary attachments or additional copying or otherwise create unnecessary network traffic. As audio, video and picture files require significant storage space care should be taken if attaching or downloading such information and it must be business-related.

4.4 It is Company policy to monitor mail to ensure that the system is not being misused. Routine monitoring by the Company will take place. Individuals should remember that items deleted from the system may still be accessed and therefore monitored. The Company may use human or automated means to monitor the use of its Information Technology resources.

4.5 As the language and style of writing of e-mails tends to be less formal, a general rule to adhere to when sending e-mail messages is that you should never put anything in an e-mail which you would not like to have read out in court. You should endeavour to make each electronic communication truthful and accurate. You must use the same care in drafting e-mails and other electronic documents as you would for any other written form of communication. You should always strive to use good grammar, correct punctuation and spelling and keep in mind that anything created or stored in the computer system may, and in all likelihood will, be reviewed by others.

4.6 Care must be taken not to commit the Company by electronic communication to any contracts and the same authorisation procedures apply as to any other form of communication.

4.7 An employee should never include in an e-mail:-

- anything which could be construed as defamatory about either an individual or Company;
- obscene or blasphemous material;
- anything which could be construed as intimidating;
- anything which is fraudulent, abusive, embarrassing or sexually explicit;
- anything which could be construed as sexual or racial harassment; or
- anything which breaches confidentiality.

4.8 Anyone encountering or receiving this kind of material should immediately report the incident to their immediate Manager.

4.9 It is important that all employees are aware that the following actions in relation to e-mail use are prohibited:

- Abuse of the e-mail system by excessive use for personal correspondence;
- Making any comment or statement which could in any way be contrived to be defamatory however innocent you consider them to be;
- Initiating or forwarding an e-mail that contains obscene or pornographic material;
- Initiating or forwarding an e-mail which could be considered to constitute an act of harassment or be discriminatory;
- Disclosing information which is protected by embargo or could in any way be considered confidential to the business and/or the employees; and
- Making any statements via e-mail which intentionally or unintentionally creates a binding contract or make negligent statements.

5 Log-Ins

5.1 The Company operates a number of its facilities by using and storing sensitive and other documentation on its Computer Software. All information related to the Company or hosted on any Computer belongs to the Company.

5.2 Subscriptions to services will only be permitted, subject to prior authorisation from the Director.

5.3 Employees are provided with Log-in details in order to access secure and protected areas of the Company's site and assets. Employees are strictly

prohibited from disclosing and revealing this information to any individual, unless permission has been granted by a Manager.

5.4 Employees should not alter passwords or create a new password or domain names to protect work without authorisation from the Director. All personal passwords must be fully disclosed to a Director upon request.

6 Sanctions

6.1 Failure to comply with the above policy may result in disciplinary action that may lead to dismissal.