“ANNEXURE I”

IT POLICY

The Dentsu Aegis Network computer policy has recently been updated to reflect changes in the way computers are used at work and complies with the latest legislation. It adds greater clarity on your rights and responsibilities, so it's very important that you read the policy in full. The document can be accessed from the User Guides section of the Group Policies page on NEON, by clicking the following link: http://neon.aemedia.com/aegis-media/policies/Documents/OP%203%20Acceptable%20Use%20Policy/OP3%20Acceptable%20Use%20Policy%20June%202014.pdf

Please see below for some of the main issues within the full policy.

1. You are provided with a computer and access to systems and applications as required for the performance and fulfilment of job responsibilities.

2. You should have no expectation of privacy while using company-owned or company-leased equipment. Information passing through or stored on our equipment can and will be monitored. You should also understand that we maintain the right to monitor and review Internet use and email communications sent or received by you and all files, stored, created or accessed on our computer systems.

3. For your protection, you are responsible for keeping your personal passwords secret. You should not disclose your password to anyone else, even if you leave the company and you must not use someone else's ID and password. You must change your password immediately if you suspect someone else knows it.

4. You must be diligent in protecting both your password and system by locking your workstation whenever you leave it.

5. We may inspect all electronic communications and files made or received by you. This may include conducting email sweeps, or accessing emails either at random or as part of an investigation from time to time. We may monitor the use of the Internet and contents of emails and files for propriety and for quality, security and audit purposes. We may access any material sent or received on email and any files stored, created or accessed on our computer systems.

6. You are allowed to access the Internet on our systems on the express understanding that you consent to us having access to and being able to view all the material on the Internet accessed by you.

7. We also reserve the right to review all use of the computer systems, including the content of network drives. You should therefore expect that we will be aware of every instance of computer usage, including that of a personal nature and Internet sites visited.

8. By using the computer systems you acknowledge we have the right to examine your user accounts for malpractice and, if necessary, to pass on data to a third party for investigation.

9. Our computer systems are primarily for business use. Occasional and reasonable personal use is permitted, provided that this does not interfere with the performance of the corporate network infrastructure, work duties and responsibilities.

10. You must only use approved hardware and software obtained through the IT Department procurement process. This includes software and “plug-ins” downloaded from the Internet.

11. If you use your own personal computer equipment to carry out work on our behalf, you must ensure that up to date virus protection is installed and that you are using licensed software.

12. The systems run software under the licence of third parties and store information about us, our clients and others, which must be protected as confidential. For those reasons use of the systems is restricted and access granted on a 'need to know' basis. Unauthorised copies of software or information must not be taken, used or transferred. You must not make copies of any computer programs or files unless these copies are reasonably necessary for the performance of your duties and do not infringe the rights of any third party.

13. Software piracy will not be tolerated in any form. This includes personal music and video files held on our computer systems. Where you choose to do this, you are responsible for ensuring that you are legally entitled to hold a copy of such files in electronic format and own the rights to do so.

14. Unless expressly authorised, you must not install, change, move or make any additions to computer systems. This includes connecting unauthorised computer equipment, for example Personal Digital Assistants (PDAs) and mobile phones to our network.

15. You must not allow unauthorised people to access or use our computer equipment, without the express permission of the IT department. This includes, but is not limited to, friends and family and suppliers.

16. You must immediately delete any inappropriate message, image, photograph, animation, movie or drawing which you may receive from outside Dentsu Aegis Network. You must not forward this type of material. You must immediately notify your manager if you should receive an inappropriate message, image, photograph, animation, movie or drawing from an individual within Dentsu Aegis Network.

17. The auto-forwarding of email to a home or other external computer is not permitted and the use of remote access software and programmes such as GoToMyPC is expressly forbidden.

18. We will not tolerate the use of the system to publish, display, store, request (download) or transmit any information that:

19. Violates or infringes another person’s rights or copyright laws.

    - Contains any defamatory, abusive, obscene, profane, sexually orientated, intimidating, threatening, offensive or discriminatory material, including where asterisks have been used to 'disguise' words that would otherwise fall under this category.

- Forges, impersonates, misrepresents, misleads or fabricates, including representing personal opinions as those of Dentsu Aegis Network.
- Is malicious, for example, computer viruses.
- May bring Dentsu Aegis Network into disrepute, for example engaging in gossip or speculation or expressing derogatory views about people or organisations.
- Spams email accounts from our email services/computer systems or is illegal in any other way.
- Is for personal financial gain or is related to gambling (except for explicit business purposes).

20. If issued with a laptop and other portable devices you are personally responsible for the safety and security of the equipment. If you are leaving the equipment on site overnight it must be locked away in a drawer or cupboard.
21. If you decide to use our computer systems for personal purposes, you do this on the understanding that you accept full responsibility and liability for any purchases, transactions and actions. We shall bear no responsibility for any damages whatsoever for any reason.
22. Each time you log-on to your computer, you will be presented with a screen that highlights this policy. This is to advise and remind you that in order to access your computer, you agree to abide by this policy. Any violation of this computer use policy, as outlined above, could result in disciplinary action being taken against you, up to and including summary dismissal.
23. The use of One Drive sync client for Windows and MacOS is forbidden for use on your home PC. Synchronising company data to your home PC could result in disciplinary action.

Please sign below to indicate you have read and understand the terms of our IT Policy and undertake to abide by it.

Signed at this day of 201...

Signature: _____

Name: _____