01. SLACK COMMUNICATION USAGE POLICY

SLACK COMMUNICATIONS

REF: CERTIFICATION of SLACK COMMUNICATION USAGE POLICY â€œAssets / The Materialâ€ owned by **Iconic Performancesâ„¢**, it associates, successors and affiliations.

Iconic Performances Pty Ltd (â€œCompanyâ€) will provide access to THE COMPANY SLACK SERVER COMMUNICATION PROGRAM (â€œAssetsâ€) that the WORKER (with refers to any person who is an employee or contractor or volunteer who has been approved to use SLACK on the Iconic Production Server for business related purposes only). will use to communicate with staff and contractors on the COMPANY SLACK SERVER COMMUNICATION PROGRAM to certain WORKERs for use in their jobs. This policy and agreement sets out the acceptable and unacceptable usage of the ASSETS.

1. The COMPANY recognises that staff and contractors need access to the ASSETS systems and the internet to assist in the efficient and professional delivery of services and communication.Â The COMPANY supports the right of staff to have access to reasonable use of the ASSETS and communications in the workplace.

2. This policy sets out guidelines for acceptable use of the ASSETS, including internet access to the ASSETS by the WORKER of the COMPANY.Â The primary purpose for which access to the ASSETS is provided to the WORKER is to assist them in carrying out the duties of their contract and/or employment

3. The Usage Policy applies to the WORKER of the COMPANY who has access to computers and the ASSETS to be used in the performance of their work. Use of the ASSETS by the WORKER is permitted and encouraged where such use supports the goals and objectives of the business. However, access to the ASSETS through COMPANY is a privilege and the WORKER must adhere to the policies concerning the ASSETS, including Computer, Communication and Internet usage. Violation of these policies will result in disciplinary and/or legal action leading up to and including termination of the contract and/or employment. The WORKER may also be held personally liable for damages caused by any violations of this policy. Â The WORKER is required to acknowledge receipt and confirm that they have understood and agree to abide by the rules hereunder.

4. The WORKER is required to provide an eligible and legally approved ID before an account is setup for the WORKER.Â The WORKER is required to provide a small photo identical to the approved ID for security and should only change the photo if permission is provided by the COMPANY.

5. Any device or computer or access to any device or computer including the ASSETS, but not limited to, desk phones, cell phones, tablets, laptops, desktop computers, and iPads that the COMPANY provides for the WORKERs use, should only be used for COMPANY business. Keep in mind that the COMPANY owns the devices and ASSETS provided and the information in these devices. If the WORKER leave the Company for any reason, the COMPANY will require that the WORKER returns the equipment on the WORKERâ€™s last day of work.

6. The WORKER is expected to use the ASSETS responsibly and productively. The ASSETS is limited to job-related activities only and personal use is not permitted.

7. Job-related activities include research and educational tasks that may be found via the

ASSETS that would help in the WORKERâ€™s role.

8. All ASSETS data that is composed, transmitted and/or received by the COMPANYâ€™s ASSETS is considered to belong to the COMPANY and is recognized as part of its official data. It is therefore subject to disclosure for legal reasons or to other appropriate third parties.Â Any document, tool or any other work produced for the COMPANY purposes, any task that has been performed for the COMPANY, or any confidential information that the WORKER might become aware of through his/her work becomes the property of the COMPANY. This information is to remain confidential even after the WORKERâ€™S departure or termination.

9. The equipment, services and technology of the ASSETS used to access the ASSETS are the property of the COMPANY and the respective associates and the COMPANY reserves the right to monitor communication and traffic and monitor and access data that is composed, sent or received through its online connections with the ASSETS.Â The COMPANY accepts that the use of the ASSETS is a valuable business tool. However, misuse of this facility can have a negative impact upon WORKERâ€™s productivity and the reputation of the business.Â In addition, all of the COMPANYâ€™s ASSETS resources are provided for business purposes only. Therefore, the COMPANY maintains the right to examine any systems and inspect any data recorded in those systems. In order to ensure compliance with this policy, the COMPANY also reserves the right to use monitoring software in order to check upon the use and content of the ASSETS. Such monitoring is for legitimate purposes only and will be undertaken where required and deemed necessary.

10. Communication, documents, and attachments sent via the ASSETS should not contain content that is deemed to be offensive. This includes, though is not restricted to, the use of vulgar or harassing language/images.Â

11. GIF images are not permitted on public work channels and are deemed non-work related.Â GIF images may be used in a Direct Message if work related or on the **#random** channel if required.

12. All sites and downloads may be monitored and/or blocked by the COMPANY if they are deemed to be harmful and/or not productive to business.

13. The installation of software such as connecting technology or other programs to the ASSETS is strictly prohibited unless approved in writing by the COMPANY.

14. Unacceptable use of the ASSETS by the WORKER includes, but is not limited to:-
    1. Distributing, disseminating or storing images, text or materials that might be considered discriminatory, offensive or abusive, in that the context is a personal attack, sexist or racist, or might be considered as harassment.

    2. Using computers and/or the ASSETS to perpetrate any form of fraud, and/or software, film or music piracy, including distributing, disseminating or storing images, text or materials that might be considered indecent, pornographic, obscene or illegal.

    3. Stealing, using, or disclosing someone else's password without authorization.

    4. Downloading, copying or pirating software and electronic files that are copyrighted or

without authorization.

5. Sharing confidential material, trade secrets, or proprietary information outside of the COMPANY and/or forwarding of COMPANY confidential messages to external locations.

6. Hacking or accessing into unauthorized websites via the ASSETS.

7. Visit and access web sites containing objectionable (including pornographic) or criminal material.

8. Sending or posting information that is defamatory to the COMPANY, its products/services, colleagues and/or customers.

9. Introducing malicious software onto the COMPAY network and/or jeopardizing the security of the COMPANYâ€™s electronic communications systems.

10. Sending or posting chain letters, solicitations, or advertisements not related to business purposes or activities.

11. Discussing, providing, forwarding matters relating to employment contracts, conditions, agreements that are of confidential material and status or discussing such matters with other workers in a public or group channel.
12. Broadcasting unsolicited personal views on social, political, religious or other non-business related matters.

13. Making copies of system configuration files, communication logs or attachments for personal use or to provide to a user external to the COMPANY is forbidden.

14. Downloading or installing security programs that reveal weaknesses in systems security of the COMPANY or its ASSETS.Â For example, the WORKER shall not run password-cracking programs.

15. Passing off personal views as representing those of the COMPANY.

16. WORKERâ€™s are not to share accounts, passwords or personal telephone numbers via the ASSETS except when specifically delegated (e.g. an absence) or approved by the COMPANY management.

17. Using the ASSETS to play games during work hours.

15. If an WORKER is unsure about what constituted acceptable Internet usage, then he/she should ask his/her supervisor for further guidance and clarification.

16. All terms and conditions as stated in this document are applicable to the WORKER of the COMPANYâ€™s ASSETS network and connection. All terms and conditions as stated in this

document reflect an agreement of the WORKER and should be governed and interpreted in accordance with the policies and procedures mentioned above. Any user violating these policies is subject to disciplinary actions deemed appropriate by the COMPANY.

17. Where it is believed that an WORKER has failed to comply with this policy, they will face the COMPANYâ€™s disciplinary procedure. If the WORKER is found to have breached the policy, they will face a disciplinary penalty ranging from a verbal warning to dismissal. The actual penalty applied will depend on factors such as the seriousness of the breach and the WORKERâ€™s disciplinary record.

18. The WORKER acknowledges they have read the policy, and understand they are responsible for complying with the policy rules.

19. The WORKER understands that violation of such policy may result in consequences including termination of the employment/agreement/contract.

20. The WORKER understands and will abide by the Communication Usage Policy and further understands that should they commit any violation of this policy, their access privileges may be revoked, disciplinary action and/or appropriate legal action may be taken.

21. The WORKER understands that if â€œASSETSâ€ are found to be in their possession, uploaded on any public domain, social media platform, internet webpage or shown externally after signing acknowledging schedule 2 without any reasonable and valid reason in accordance with the signed Agreement, they will be in breach of the agreement and the Corporations Act of 2001 in NSW Australia and can be prosecuted to the full extent of the law for loss of income, damages and illegal use of property and confidential information.

Unique solution ID: #1301
Author: John Khoury
Last update: 12-Apr-2019 07:03