ELECTRONIC MEDIA USAGE POLICY

Purpose:

Octopus's electronic media and communications systems are provided by the business as a tool to enhance efficiencies and communications between Clients and Employees. These systems also have the potential to cause significant problems if misused.

It is essential to Octopus that its systems are not used in any way to engage in conduct that is discriminatory, or to access, store or distribute any material that is offensive, defamatory, harassing, or in breach of its obligations to maintain privacy.

Octopus has accordingly created this Electronic Media Usage Policy to:

(a) Educate authorised users in respect of the proper standards of use of the Octopus Electronic Media and Communications Systems

(b) Strictly prohibit the inappropriate use of those systems

(c) Advise authorised users of the Octopus electronic media and communications systems of the consequences of failing to abide by the appropriate standards of behaviour set out in the Policy

(d) Safeguard the interests of Octopus and the authorised users of Octopus's electronic media and communications systems.

Scope:

This Policy applies to all authorised users of the Octopus electronic media and communications systems including all Octopus Employees, contractors and customers.

This Policy comes into effect on 1 April 2017; however, Octopus reserves the right to change the contents of the policy in the future.

Any questions, comments or concerns about the contents of this policy should be directed to the HR Manager or General Manager of Information Technology and Communications.

It is the responsibility of **all** Employees to ensure that the appropriate behaviour is conducted in the workplace at all times.

"We take our responsibilities seriously and so should you"

Policy:

All Octopus personal computers, thin clients or electronic media are to be used only for authorised business purposes. Although we do not however, wish to create a sterile environment and recognise that personal use may occur from time to time. Any such reasonable use must not interfere with your work performance, involve conflict of your duties to Octopus or other Octopus Employees, or involve breach of any other term of this Policy. Octopus reserves the right to withdraw this privilege at any time without notice.

1. Prohibition

   All forms of **offensive material** and **inappropriate use** of electronic media are strictly prohibited.

   Offensive material is not limited to but shall include any material that is fraudulent, unlawful, harassing, sexually explicit, pornographic, obscene, violent, disparaging, vilifying, hateful, intimidating, defamatory, containing sexual comments relating

to a person's gender, age, sexual orientation, race, religious or political beliefs or other any sites deemed illegal by local, state or federal laws.

Inappropriate Use As an authorised user of Octopus's Electronic Media and Communications System, you must no under any circumstance: -

a) Knowingly access or receive any offensive material through the electronic median and communications system
b) Store of fail to delete or dispose of any offensive material that is received through the electronic media and communications systems
c) Create any offensive material
d) Display or print any offensive material
e) Send, forward or disseminate in any way whatsoever any offensive material through or by the electronic media and communications systems
f) Send, receive, print or otherwise disseminate proprietary data, trade secrets or other confidential information of the business with other companies or organisations
g) recording of private conversations without consent
h) Breach any obligations of confidentiality, intellectual property and/or privacy of or any other person or company belonging to Octopus.
i) Attempt to read, delete, copy, or modify the electronic mail of other authorised users without their express permission
j) Use the media to gain unauthorised access to, modify or corrupt data stored on or sent via the Octopus Electronic Media, or damage the integrity of the Octopus media systems or systems of others in any way
k) Forge (or attempt to forge) email messages
l) Use the systems and/or networks in an attempt to gain unauthorised access to remote or local systems.
m) Breach the law in any other way

What should I do if I receive inappropriate media?

a) Should an authorised user receive any form of inappropriate or offensive material, it must be deleted immediately. If you have any concern or questions relating to the material, you should contact the HR Manager or General Manager of Information Technology and Communications as soon as possible.
b) Any authorised user found to have transmitted; re-transmitted, copied printed or stored such material will be subject to disciplinary action.

2. Monitoring

All Octopus Electronic Media is hosted by Trusted Cloud and as such may be monitored on an ongoing basis to ensure that the electronic media and communications systems are properly used and inappropriate usage of these systems is not occurring.

By signing this policy you agree that Octopus may monitor, access or record any of the files, email or internet sites that have been visited by you as an Employee of the firm to ensure Email and Internet use is appropriate and professional.

This monitoring will be continuous and ongoing during your employment with the business and will commence from the date of signing this policy for all current Employees and the date of commencement for all new Employees.

Trusted Cloud is responsible for monitoring any potential misuse of email, internet and intranet services, as well as protecting Octopus's computer network and systems from any unauthorised external access to these facilities.

Monitoring activities include:

a) All web access logs
b) Web usage statistics on a regular basis
c) All outgoing/incoming email messages

d) Email addresses of those with whom users have communicated
e) Random checking of computer hardware

3. Social Media Policy

This policy provides guidance for employee use of social media, which should be broadly understood for purposes of this policy to include blogs, wikis, microblogs, message boards, chat rooms, electronic newsletters, online forums, social networking sites, and other sites and services that permit users to share information with others in a contemporaneous manner.

The following principles apply to professional use of social media on behalf of Octopus Hospitality as well as personal use of social media when referencing any of Octopus Hospitality's clients.

a) Employees should be aware of the effect their actions may have on their images, as well as Octopus Hospitality and Octopus Hospitality's Clients image. The information that employees post or publish may be public information for a long time.
b) Employees should be aware that Octopus Hospitality may observe content and information made available by employees through social media. Employees should use their best judgment in posting material that is either inappropriate or harmful to Octopus Hospitality's client company's image, employees, or customers.
c) Although not an exclusive list, some specific examples of prohibited social media conduct include posting commentary, content, or images that are defamatory, pornographic, proprietary, harassing, libellous, or that can create a hostile work environment.
d) Employees are not to publish, post or release any information that is considered confidential or not public. If there are questions about what is considered confidential, employees should check with the Human Resources Department and/or supervisor.

Any breaches of your obligations may result in exclusion of future shifts and/or potential termination from Octopus Hospitality.

4. Confidentiality and Privacy

Octopus handles a large volume of material that is confidential and private to the business, our Employees, customers and suppliers. It is crucial that the confidentiality and privacy of this material is preserved at all times.

5. Integrity of Systems

Octopus relies on the integrity of its electronic media and communications systems and the information stored on them, and needs to be sure that its systems are not being inappropriately used. The following rules apply for all authorised users: -

a) Authorised users are responsible for ensuring their accounts and passwords are kept confidential and must not use other authorised users' account or their equipment without the other authorised users' express permission
b) As an authorised user you are responsible for the confidentiality of your accounts and passwords and must take all reasonable care to ensure that the confidentiality is maintained. In particular, you must not share your account details or password with any other authorised user, unless expressly permitted by Octopus.
c) You should take further care not to leave your email or intent account open while absent from your computer.
d) Authorised users should not use systems to damage, modify, impair, or compromise the security of the Octopus systems or any other system, such as but not limited to:

    i) Introducing or allowing a virus to be introduced
    ii) Copying or downloading software without prior approval from management
    iii) Interfering with the software or operating parameters of the Octopus Network
    iv) Using systems to gain access to information on a Octopus computer of another device or computer network without authorisation

e) Only Employees of Octopus may have access to the Octopus network unless approval have been granted by management
f) Use of the Internet for private business purposes must have approval from management
g) The Internet is not secure, any secret, proprietary or private information of Octopus must not be sent over the internet unless it has been encrypted by approved methods. Security must never be compromised. Contact Trusted Cloud regarding approved encryption methods

6. Best Practice

E-mail is considered correspondence from the business and has the same legal implications for both the sender and the business as correspondence on letterhead and should be treated accordingly.

a) Standards for writing emails
    i) The Octopus Style Guide should be followed to ensure all electronic media correspondence meets the business's standards
    ii) Emails should never be written in Capitals as it LOOKS LIKE YOU ARE SHOUTING
    iii) Be aware of your audience and write as if it's a letter
    iv) Don't write anything you wouldn't be comfortable seeing in the papers the following day
    v) Make them short
    vi) Use salutations
    vii) Mare sure they have a disclaimer

b) All e-mailed Marketing communication (invitations, newsletters, surveys etc.) must contain an unsubscribe option.

7. Breaches of this Policy

Allegations of any failure to comply with the requirements of this policy will be treated seriously by Octopus.

Where a breach of this Policy is alleged, Octopus will review and investigate the conduct on an individual basis

A finding that a breach of this Policy has occurred will lead to the appropriate disciplinary response which, depending on the circumstance and seriousness of the breach, may include

a) Warning
b) Suspension of the person who has been guilty of the breach
c) Reassignment or demotion
d) Termination of employment with or without notice

8. Email Disclaimer

The following disclaimer should be placed within your email signature and attached to all emails that are sent external authorised users:

"The information transmitted is intended only for the person or entity to which it is addressed and may contain confidential or privileged material. Any review, retransmission, dissemination or other use of, or taking of any action in reliance upon, this information by persons or entities other than the intended recipient is prohibited. If you received this in error, please notify the sender and delete the material from your computer."

"SAVE PAPER - THINK BEFORE YOU PRINT"

"Supporting Paperless Office Concepts"

9. Definitions

The following definitions apply to this Policy:

Electronic Media and Communications Systems refers to any equipment through which information is transmitted electronically. It includes the use of computers, laptops, thin clients, servers, smart phones, email, mobile phones, SMS messaging, voicemail, fax machines, wireless devices, printers, online services, the Internet and any media capable of receiving, transmitting, storing information, text or images.

E-mail refers to all forms of electronic mail and electronically based messaging sent and received on Octopus computers and networks.

The **Internet** is a world-wide system of computer networks in which authorised users and any computer can, if authorised, obtain information from any other computer and/or talk directly to authorised users at other computers.

Authorised user is any Employee, agent of contractor of Octopus or a related company who has been given authority to use its electronic systems for an authorised business purpose.

Authorised Business Purpose is a legitimate purpose which is directed to the advancement of the business interests of the organisation by lawful means.

Related Policies:

- Code of Conduct
- Employee Privacy & Confidentiality

Related Forms:

- Orientation Form