“Your Company Name”

EMPLOYEE IT AND INTERNET USAGE POLICY

Employee IT and Internet Usage Policy

1. Overview

The significant potential for misuse of personal information and the potentially costly reporting requirements in the event of unauthorised disclosure or access to information require us to make sure that we (and you) take our IT and Internet usage seriously.

As a responsible data custodian, and in order to make sure that our client's personal information is kept confidential and secure when we use the internet, computers and other electronic devices and equipment, "Your Company Name" requires all its employees, contractors, external agents, representatives and anyone else who accesses our network and computers, to abide by this Employee IT and Internet Usage Policy at all times when at work, when using workplace provided devices, or when accessing our systems.

When using "Your Company Name" accounts you are acting as representatives of "Your Company Name" and any inappropriate or unlawful activity may be the responsibility of the firm. As such, you should act accordingly to avoid damaging our reputation. We are a professional business and must always act professionally. We may choose to hold you liable for any unlawful or inappropriate actions you take.

2. Access to our IT systems

Our IT system may only be accessed when you are on the premises of the firm, however certain personnel can gain access to the system remotely. Our IT system may only be used by employees or contractors of the firm for firm business.

Staff must not place any of our firm material (including copyrighted software, confidential information, internal correspondence etc.) on any publicly accessible website or computer without proper permission.

Any devices that connect to our IT systems must be secure and have security protections in place (for example PIN codes, thumbprint identification, up-to-date software, applications and anti-malware software, strong passwords)

3. Computer Viruses

Each team member is responsible for downloading and keeping virus-checking software for your computer system up to date. Do not modify this software without managerial notification and approval.

Computer viruses can destroy computer systems by wiping all the data stored on them, corrupting files, and damaging software programs. Imagine what it would be like if you came in to work tomorrow and all your work for the last month was gone! We need to avoid computer viruses at all costs.

Computer viruses enter the system from an outside source. This may be via:

- email messages.
- email attachments.
- a CD-ROM/DVD.
- a USB drive; and/or
- another form of portable storage device.

To avoid introducing viruses to the system, the following procedures must be followed by all our employees, and contractors.

No external storage devices (USB drives, portable hard drives etc.) may be put into any computer in the office unless these have been virus checked and initialled & dated as such by the computer user.

Only standard Word and Excel attachments from clients may be opened. NO other attachments, such as jokes, graphics etc. may be opened. These must be deleted immediately as they are much more likely to contain programs that have viruses in them.

If a virus warning shows on your computer screen, you MUST NOT proceed. Close the item totally and ask Preston Wong to assist you. Your computer may be able to be "cleaned" or you may have to contact the client and ask for another copy.

4. Personal use of our IT system

The firm takes no responsibility for any personal data you may have on the system or the infection of any personal devices by any malicious software which has been compromised as a result of inappropriate staff use of our systems.

As all information on the computer system is the property of the firm, we may read, delete, alter or use this information at any time.

5. Passwords and Logins

For passwords and logins of all computers see "team lead name". Do not share your password with anyone else. Passwords must be strong, and always be kept secure and secret. Passwords must not be simple, easily cracked words or numbers (eg. Password1). The same password must not be used for your work logins that is used for your personal logins.

Strong passwords are those with at least six characters, and a combination of lower and uppercase letters, together with numbers and symbols.

Passwords are not to be stored in easy to find locations (for example on a sticky note attached to the monitor of the computer).

If a password needs to be conveyed to another authorised person, it should only be done in person or by telephone (provided their identify has been verified), and not by email.

Passwords should be changed every 3 months.

Staff are only to log into their work accounts from safe devices.

6. Email

Emails

We use “Your companies tool” as our electronic mail system. Access to email has been provided as a business tool to make handling your work more efficient and effective.

Where possible, staff are encouraged to use “name your systems here” as opposed to using any other form of communication.

Any email received that looks unusual or suspicious, even if an internal email sent from another staff member, must be verified with the sender before opening any attachments. When in doubt, do not click a link in an email directly, go through the official website.

Do not send credit card information, client names, email addresses, or other highly confidential information through email. Consider using a secure file transfer system that will encrypt the information and only allow the authorised recipient to access it.

Sending emails and attachments to clients

No document may be sent to a client or anyone else via email without prior manager approval. This is to ensure only authorised documents are sent out and that they are sent out in the correct format. Please see your responsible manager if you have any questions.

Storage of emails – client files

Emails related to files should stored in “your companies repository”.

This includes both incoming and outgoing email correspondence, and any relevant internal correspondence.

Personal use of email

Email is not to be used for personal purposes. Personal emails should be handled on your own time (i.e. before and after work or at lunch times) and not during normal working hours.

Further, work email addresses must not be used to:

- register on illegal, unsafe, or suspect websites or services;
- send unauthorised, obscene, offensive or discriminatory messages or content.

Under no circumstances are any attachments sent by friends or unknown people to be opened – they are to be deleted immediately. As you would understand, viruses enter the system often via attachments. Viruses can destroy or disrupt our entire computer system and mean a total loss of data and software.

7. Internet

Anything sent via the Internet cannot be guaranteed to be kept private or confidential. Any sensitive material transferred over the Internet may be at risk of detection by a third party. Staff must exercise caution and care when transferring such material in any form and must follow our Privacy Policy as well as this policy in order to protect our data.

The Internet is accessible via the computer system and is for official “Your Company Name” work use only. It is not to be used for any other purpose, and only work related or otherwise authorised sites may be visited during work hours.

Notwithstanding the above paragraph, staff can access websites of their choice during work hours, but must at all times exercise good judgment, remain professional at all times and in all communications, and remain productive at work while using the Internet.

Any files that are downloaded from the Internet must be scanned with virus detection software before installing or execution. All appropriate precautions should be taken to detect for a virus or other malware and, if necessary, to prevent its spread. We may install anti-virus or encryption software on our computers. You must not deactivate or configure any settings (including in relation to firewalls) without managerial approval.

The accuracy or otherwise of information on the Internet and in email should not be considered verified until confirmed by a separate (reliable) source or by separate means (ie. telephone).

Staff are authorised to access the Internet for personal business after work hours, in strict compliance with the other terms of this policy.

Staff must not use our systems or network to do any of the following:

- Send any client information, or other confidential information, to any unauthorised recipients.
- Download or upload obscene, offensive or illegal material, or illegal movies, music or other copyrighted material or software.
- Visit any websites that could compromise the safety of our systems and computers.
- Access without authority another person’s private or sensitive information or perform any other unauthorised or illegal actions like fraudulent activity, hacking, trafficking in illegal goods etc.

The firm reserves the right to periodically check the Internet usage records to ensure that staff are not wasting firm time by visiting non-work-related sites or using the Internet for any of the above purposes.

Intentionally accessing any sites which breach any of the firm’s policies or infringe on the legal rights of others, or the introduction of viruses or malicious tampering, is expressly prohibited and could lead to the immediate termination of your employment contract.

Examples of such sites are those which include nudity, pornography, obscene language, racist images or violent images. Such behaviour will not be tolerated at “Your Company Name”

“Your Company Name” reserves the right to block access to internet sites. This might be due to the content, the risk of viruses or the bandwidth graphic/media-rich sites utilise.

8. Work-issued equipment

Work-issued equipment must be respected and protected by staff. This includes work-issued phones, laptops, tablets, portable hard drives, and any other electronic equipment.

This work-issued equipment belongs to “Your Company Name” at all times. When not in use the work-issued equipment must be securely stored. Staff are responsible for their work-issued equipment whenever it leaves our premises.

9. Privacy settings for social media accounts

Staff are highly recommended to apply the maximum privacy settings on any of their social media accounts, to make sure that only known contacts can see their personal information such as birth date, location, contact details etc. This is in order to limit the amount of personal information that is available online so that any vulnerability to a phishing attack or identity theft can be reduced.

10. Reporting of security incidents or suspicious activity

Scams do not just happen through email or the internet, they can also happen over the telephone. Do not provide confidential information to persons over the telephone or via any other method of communication unless you have verified their identity and you have verified that they are authorised to request the information they are requesting.

Staff must use common sense and take an active role in contributing to our security. Any security incidents or suspicious activity regarding any client personal information or work information must be immediately reported to Mark Kennedy This is so we can try and quickly do something to minimise any damage. Do not attempt to correct any security issues yourself as you may destroy important evidence needed to determine the extent of a problem or its type or source.

If you lose or have stolen any work-issued equipment or other device that has access to our systems, you must immediately report these as lost or stolen to “assigned team lead”. Early discovery of lost or stolen devices can make all the difference in protecting our and our client’s information.

11. Consequences of contravening these procedures

Your good judgment and common sense are essential to protecting your, our, and our client’s, systems and information.

The computer system is a vital tool in keeping the firm running efficiently and effectively. Due to the severity of the damage viruses and other inappropriate or illegal behaviour can cause, any actions you take which contravene any part of this policy could lead to serious disciplinary action or even your employment with the firm being terminated, or other legal action.

12. Employee confirmation and consent to this policy

I confirm I have read “Your Company Name” Employee IT and Internet Usage Policy and agree to abide by it as consideration for my continued employment or engagement by “Your Company Name” I understand that breaching or violating any of the above terms may result in my termination.

……..
Signature – employee/contractor

……..
Name of employee/contractor

Date: