IT Policy

Academy for Healthcare Science

Version No: 2.0 - Release Date: 04 July 2019

Prepared by: Mark Dixon

Contents

Definitions

Further references to 'AHCS', 'The Academy', 'Academy' or 'Academy for Healthcare Science' are one and the same thing in referring to the organisation that legislates this policy.

Introduction

The Academy provides you with access to various computing appliances and systems ('the Facilities') to allow you to undertake the responsibilities of your position and to improve internal and external communication. This Policy sets out the Organisation's policy on your use of the Facilities and it includes:

- your responsibilities and potential liability when using the Facilities;
- the monitoring policies adopted by the Company; and
- guidance on how to use the Facilities.

This Policy has been created to:

- ensure compliance with all applicable laws relating to data protection, information security and compliance monitoring;
- protect the organisation and its employees from the risk of financial loss, loss of reputation or libel;
- ensure that the facilities are not used so as to cause harm or damage to any person or organisation.

This Policy applies to the use of:

- local, inter-office, national and international, private or public networks (including the Internet and Intranet) and all systems and services accessed through those networks;
- desktop, portable and mobile computers and applications (including personal digital assistants (PDAs);
- mobile telephones (including the use of WAP services);
- electronic mail and messaging services.

Observation of this Policy is mandatory and forms part of the Terms and Conditions of Employment. Misuse of the Facilities will be treated as gross misconduct and may lead to dismissal.

Computer Facilities - Use of Computer Systems

The Academy has a policy that allows the use of Academy supplied PC's/laptops/tablets for both personal and business. This has been made available by separating logins on a machine and needs to be used as follows:

Personal

This is a personal login and the password is only known by you and the supplier of the password. This password can be changed and the profile (desktop) you log in with is for personal use – OneDrive, online banking, documents, Email, etc.

N.B. The device is still the property of the Academy, and as such, you will be responsible for the removal of personal belongings if the device is required elsewhere or when returned on termination of your contract.

AHCS

This login is an AHCS login and has been setup for use with the Office 365 system. In order to maintain the confidentiality of information held on or transferred via the Organisation's Facilities, security measures are in place and must be followed at all times. A log-on ID and password is required for access to the Organisation hardware and email system. You are responsible for keeping your password secure. You must not give it to anyone, including colleagues, except as expressly authorised by the Organisation. If you suspect your password is known by someone else, then you are obliged to inform the IT Supplier. Organisation passwords should only be shared with your IT Supplier or the Chairman.

Management will ensure that employees can see and if necessary challenge results of any monitoring. It is the Employer's responsibility to have the consent of both senders and receivers. Except for ascertaining regulatory compliance, detecting unauthorised use or to prevent criminal activity, personal email can only be monitored in exceptional circumstances, e.g. to investigate criminal activity (reference: 'ICO Data protection: the employment practices code').

You are expressly prohibited from using the Facilities for the sending, receiving, printing or otherwise disseminating information which is the confidential information of the Organisation or its clients other than in the normal and proper course of carrying out your duties for the Organisation.

In order to ensure proper use of computers, you must adhere to the following practices:

- anti-virus software must be kept running at all times;
- all portable media storage (CD's, DVD's, flash drives, external hard drives, etc.) must be checked for viruses
- obvious passwords such as birthdays and spouse names etc. must be avoided. The most secure passwords are random combinations of letters and numbers;
- when you are sending data or software to an external party by portable media (CD, flash drive, etc.) always ensure that they have been checked for viruses before sending;
- all files must be stored on OneDrive as this is the only storage that is backed up regularly to avoid loss of information;
- devices must not have any software/firmware installed which is designed to bypass security systems.
- large emails (over 15MB) being sent to internal distribution groups will clutter up the system so where possible please use a shared area to host the file and advise the distribution group of its location;
- emails to and from outside sources should be restricted to 15MB; which is the limit set by most Email Exchange and ISP's by default. If you have to send via email then you will need to compress the attachments or break it down into smaller quantities;

- If there is a need to purchase software for you to accomplish you job, contact the IT Supplier or your manager; and
- you should not install any proxy, DHCP, routing or VPN software other than those supplied by the IT Supplier.

Personal Equipment Usage

Some staff and contractors will not have access to equipment supplied by The Academy but will require access to The Academy's data systems. As IT have no control of personal equipment and cannot vouch for the security of said systems we can't give access in the same way. Access to emails can be achieved by webmail: https://outlook.office365.com and the files can be accessed by the Sharepoint website. We ask that you adhere to the following practices:

- Your Academy password should be secure - obvious passwords such as birthdays and spouse names etc. must be avoided. The most secure passwords are random combinations of letters and numbers;
- all files must be stored on Sharepoint and not downloaded to personal devices. We accept that you will have files you are working on and request you download a COPY and overwrite it when you upload after.
- large emails (over 15MB) being sent to internal distribution groups will clutter up the system so where possible please use a shared area to host the file and advise the distribution group of its location;
- emails to and from outside sources should be restricted to 15MB; which is the limit set by most Email Exchange and Internet Providers. If you have to send via email then you will need to compress the attachments or break it down into smaller quantities;
- When you depart company with The Academy It is your responsibility to ensure that all data own by The Academy is returned and wiped of all your personal devices.

Monitoring of System Usage

Communications (e.g. emails) or stored information may be monitored. Such monitoring is in place to ensure that the Organisation is proactive in:

- maintaining the confidentiality, integrity and availability of its systems;
- being compliant with the laws of the land and Academy policies; and
- identifying and controlling the presence of offensive, hateful or abusive content on its systems and/or mobile devices.

Such monitoring is not intended to invade the personal privacy of Academy staff. However, you should still consider the presence of such monitoring before placing your own sensitive personal information on an Organisation system unnecessarily.

Accessing of emails and secured documents (including forwarding of emails or direct account access) can only be done with the permission of the Chairman.

Investigations

A specific individual's activity will only be investigated in detail where there are reasonable grounds to suspect that the individual is contravening this IT Policy or committing a gross dismissal offence. This would only normally occur where there has been a specific complaint received or where routine monitoring has identified the individual's usage as being of potential concern. In such cases the user will not be notified at the time of collecting evidence but will be made aware afterwards. Such investigations will need approval from the Chairman and may involve the Governance and Scrutiny Committee.

Acceptable Personal Use

Staff are permitted to use company computing facilities in their own time for personal use.

Do not:

- Perform non-work related activities within paid time;
- Generate, circulate or distribute the following types of information on a Company email system or shared working environment (e.g. Microsoft SharePoint):
    - 'for sale' or 'goods wanted' type messages;
    - any message or notice intended to promote, increase awareness of, or gather support for, a political, religious or 'protest' cause or campaign. (note: this excludes any messages related to Trade Unions or Company endorsed charities and societies);
    - any unauthorised data encryption products.

- Create a user account or auction on an Internet auction site (e.g. eBay or QXL) which uses an Academy email address, postal address or phone number in the contact details.

Additionally, do not:

- put business information at risk by not having it backed up
- use personal email boxes for communicating on behalf of the Academy, e.g. GMAIL, HOTMAIL
- introduce any data to the Academy's PC, SharePoint or OneDrive without first virus checking it.
- introduce into Academy's SharePoint or OneDrive system, any executable file downloaded from the Internet.

If in doubt consult the IT Supplier.

Inappropriate or offensive content

Under no circumstances should you install, generate, browse, download, store or transmit content (images, video, sound, text messages etc.) that is inappropriate or offensive. This includes scenarios such as transmission from an Organisation's computer system, transmission to an Organisation's

computer system (e.g. from a personal email account) and transmission entirely within the Organisation's storage systems.

The following content is considered inappropriate or offensive (as a minimum):

- content referring to other individuals that may embarrass or humiliate them;
- content of a sexual/pornographic nature which could cause offence;
- content of a racially related nature which could cause offence;
- content relating to personal disability which could cause offence;
- content of a religious nature which could cause offence.
- content that may be linked with international terrorism/radicalism, etc.

Use of the Academy's computers, telephone lines, telephone systems, Internet connection or any other system or software or equipment owned or controlled by, leased or rented to us to access Internet sites or download or receive email or other electronic images or media that contains pornography or other obscene or illegal contents shall constitute gross misconduct that can lead to your dismissal without notice.

Ensure that what you do is legal.

Examples of how you might break the law, or result in the Academy (or organisations working with the Academy) breaking the law, are:

- using social media (Twitter, LinkedIn, Facebook etc.) in an inappropriate way;
- installing, copying or using unlicensed software or loading or downloading of illegal music or audio files;
- gaining unauthorised access to computing facilities in contravention of the Computer Misuse Act 1990;
- not complying with the requirements of the Official Secrets Acts 1911-1989;
- not complying with the requirements of the Data Protection Acts 1984 & 1998;
- not complying with Copyright legislation;
- transmitting material in breach of confidence (e.g. contrary to a non-disclosure agreement);
- transmitting or storing material that is likely to be defamatory, to cause loss, damage or harm, to cause offence, or to be a nuisance;
- transmitting data across national borders, contrary to any export control restrictions.

Note: this list is not exhaustive.

Data Security / Breaches

Disabling of virus software is not permitted. The antivirus software may be temporarily disabled to enable installation of software approved by the IT Supplier. Antivirus software updates must be conducted regularly and automatically where possible.

Only download 3rd party software with permission of your manager, being wary of accepting 3rd party agreements (some of these give permission to download free malware, pop-ups, etc…)

If your data device acts suspicious, in any way, as a result of opening an email attachment or installing software, or you have multiple pop-ups, remove the device from the network (pull out network cable and/or disable wifi) and report the incident to your manager or IT supplier.

Your password to access the PC is also the same password to access the companies email via cloud/internet services, it is therefore your responsibility not to share that password with anyone (unless explicitly requested by your manager) and you should ensure you change your password if you suspect it maybe compromised.

Social Media

The Academy should not be identified in any social networking sites such as Facebook and YouTube etc. You should always endeavour to preserve the 'good' image of the Academy in your use of computing facilities. Examples of how you can do this are:

- ensure that the wording of all communications is professional, factually correct and not excessively informal or inappropriate;
- ensure that the appropriate format, punctuation and spelling is used in formal documents or external communications;
- ensure that the intended recipient's details are correct (especially with email).

Mobile Devices (tablets, smartphones, etc.)

New technology allows organisation email accounts to be linked to these devices and the policy of the Academy is that if the device is not company owned then is should not hold company data unless permission is given from a Manager. The Academy's email system logs these devices and when you first login will add a policy to your device that allows the Academy to wipe it; therefore if you set up an Academy email account (excludes a web browser to OWA) on any device, the Academy retains the right to wipe the device to ensure protection of organisational data.

In the event of loss of any mobile device storing the Academy information it is essential that you:

- change your logon password immediately;
- use the 'Find my iPhone' or equivalent service to erase the device immediately;
- report the incident to the IT Supplier as soon as possible.