Policy title: KOA ICT Security Policy
All-through
Date adopted: 13 November 2017

Version	Date	Page	Change	Origin of Change *E.g. change in legislation*
V 1.0	19 September 2016			
	November 2017		No Change	

Link to other policies:
KOA ICT Acceptable Use Policy

Terminology
We use the term Information and Communications Technology (ICT) to reflect the close integration that now exists between computers, data networks, and telephony systems. On some occasions we continue to use the term IT for ease, or because people are used to it.

Welcome to the ICT Security Policy
ICT security is essential to protect the Academy's investment in hardware, software and data. It also reduces the risks of fraud and inappropriate access to confidential data. The Academy relies on its data network, which we do a great deal to secure and protect.

Everyone who uses the Academy's ICT systems and equipment must read, understand and comply with this Policy.

Every ICT user must take security issues seriously. Even if you consider yourself a small and unsophisticated user you could be the channel by which a virus is introduced, or a hacker gains access to our systems.

Why ICT Security is Important to You
You would not leave your car unlocked and the keys in the ignition; or tell a complete stranger in the street your home address and then hand over your keys; or write your PIN on your credit card.

Yet surprisingly some people do very similar things when it comes to IT systems. Writing passwords on Post-Its, letting colleagues log in as you, loading untested software and many similar practices are equally risky.

This Policy gives very similar guidance for IT systems. It's a list of basic good housekeeping that **everyone must observe**.

Where appropriate we have tried to explain why these requirements exist. But the risks are so many and diverse that we can't cover them all.

For example, most people have heard of viruses and understand that they can cause a great deal of damage and inconvenience. But there are other risks, such as hidden bits of software that secretly record all your keystrokes and then send them to an unknown third-party.

The advent of the Internet has also changed the boundaries of ICT systems. Malicious people can attack from anywhere in the world, and information you might think harmless or trivial can be a key advantage that they can exploit.

Finally, observing this Policy is a formal requirement for all members and staff. Breaking it will be regarded and may be treated as a disciplinary offence.

1. Scope

This policy applies to all staff, including part-time, temporary staff and agency staff.

ICT Systems include: -

1. Hardware
2. Software
3. Data networks
4. Data

2. Terms and Definitions

Information Security means preservation of the confidentiality, integrity and availability of information.

- Confidentiality – ensuring that information is only accessible to those authorised to have access.
- Integrity – safeguarding the accuracy and completeness of information and processing methods.
- Availability – ensuring that authorised users have access to information and IT assets when required.

It is the responsibility of managers to ensure that equipment is held securely. When staff leave managers must ensure that any equipment issued to that individual is returned so that the ICT inventory can be updated appropriately.

3. Personnel Security

New Staff

All new staff will be issued with guidelines for ICT access and use, a summary sheet of the ICT Security Policy, an 'ICT New Starter Request Form' and direct access to the full ICT Security Policy in the staff shared area.

Staff will be informed that they must read the Security Policy, confirm that they have read this and will comply with the Policy.

Note this includes agency staff and consultants who require using the Academy's IT systems.

Responding to Security Incidents

If you are aware of or suspect any action that is contrary to this Policy you must report it as soon as possible to the ICT team on extension 2291.

All Staff
Aware and need to sign agreement of adherence.
Staff training for all about best practice and security dangers.

4. Physical and Environmental Security

Equipment Security
Equipment should be located as securely as possible, so as to minimize the risk of potential threats, including: -

- Theft
- Fire
- Smoke
- Water
- Dust
- Vibration
- Electrical supply interference

Please ensure you log off and shut down your PC at close of day.

Security of Equipment Off-Premises

Laptop Computers: Particular care should be taken to ensure the safe custody of laptop computers.

Staff will be responsible for the safekeeping and insurance of ICT equipment when taken home.

Equipment and media taken off Academy premises must

- Not be left unattended in public places
- Not be left in an unattended vehicle
- Be carried as hand luggage and covered or disguised where possible when travelling

Computer Suites

- Management of Classes / Pupils taken into the ICT suites for lessons: Rules should be observed so that Pupils treat the equipment with respect and leave it in readiness for the next users.
- Please report any abuse of equipment a.s.a.p. to the ICT team or a member of SMT.
- Health & Safety notices of No Food or Drink in the computer suites must be observed.

There is a separate Student ICT policy, which is part of the home/Academy agreement that reinforces ICT rules.

5. Communications and Operations Management

Licensing
Users who buy software are responsible for ensuring that the software licence is held securely and available for verification. This should be through the ICT department, in consultation with departmental heads.

Unauthorised Software
Users must not make unauthorised copies of software, or download or install unauthorised software. Further, users must not accept screen prompts to download and install 'unsigned' ActiveX controls via their Internet browser.

- The execution of specific programmes can be disallowed through the operating system.

Viruses
All users must be aware of the risk of viruses, and the serious damage they can inflict. Although we use anti-virus software extensively, new strains are constantly emerging so there is no room for complacency.

Do not pass on virus warnings to other people. Many are hoaxes, designed to cause disruption in precisely this way.

Do not act on warnings that suggest you delete files from your PC. They usually suggest that you delete files essential to the working of your computer.

Please exercise care when transferring files via floppy discs, CDs and memory sticks. This is particularly important if you are working on a home PC and transferring the results to your work PC. Where possible please e-mail such files, as in this way they will be subject to virus checking. However, files over 5 Mb will be rejected.

Attachments to e-mails are a common and easy way to spread viruses. Do not: -

1. open any attachment from a source that looks in any way suspicious (particularly unsolicited e-mail).
2. open any attachment with a name that ends in .com, .exe, .sys, .dll, .bat, .avi, .mov, .kak, .shs, .mp3 or .wma.

- If you are at all suspicious do not open attachments. Seek guidance from the ICT Office on 2291.

Backups
Save all the files you create on the network. Servers are regularly backed up, so your information will not be lost if your PC is damaged or stolen. You will also be able to work on another PC if your own breaks down.

When working with databases, spreadsheets and other files that contain important data make regular backups. This will help you recover if you make an accidental mistake that deletes or damages your data.

The Internet
Be aware that information passed across the Internet is not generally secure. This includes e-mails sent to external addresses. Files and e-mails might be intercepted, or can easily be mis-delivered if you make an error in an e-mail address.

Do not use the Internet for highly sensitive data.

6. Access Control

User Access Management
New users will be set up on the network on receipt of an 'ICT New Starter Request Form' (given out at the same time as the ICT Security Policy rules and ICT guidelines). This form needs to be completed and given to the ICT team

When staff leave the Academy's employ, all their user network access will be closed.

When agency and contract staff leave, line managers are required to inform the ICT Team.

Passwords
Passwords are the front line of computer security and require particular attention.

You are responsible for actions undertaken with your password.

Do not disclose your password to anyone. Literally no one. Do not allow other members of staff to know your password, or allow them to use the access it provides.

Managers do not have a right to ask you for your password. If you need to share information this can be done in a proper and controlled way. We will work to help you achieve it.

- Passwords should be changed on a regular basis, e.g. every term.

Select passwords with a minimum of six characters and at least one number (e.g. ersatz1).

Don't
- Choose 'easy to guess' passwords.
- Write your password down unless you can hold it securely.
- Include your password in any automated process, such as a macro or user defined function key.

Avoid passwords based on

- months of the year; days of the week, or other aspects of the date.
- family names.
- car registration numbers.
- company names or references.
- telephone numbers.
- user identification names.
- more than two consecutive identical characters.

Acronyms can be used to generate passwords. For example, ic2wbc for I Come To Work By Car, or HIGN4U for Have I Got News For You. Make your own up – don't use these!

If your password has been compromised in any way contact the ICT team immediately to have it changed.

Access to the Internet

You must not connect any PC, laptop or mobile device to the Network without authorisation from the ICT Division.

We maintain a protection system (known as a firewall) to protect the Academy's network from external threats. The use of private accounts can circumvent this protection and pose a threat not just to the item affected, but also to the entire network. This is particularly the case with laptop computers.

ICT staff will immediately disconnect or disable any device that is suspected to be unauthorised.

7. Compliance

Computer Misuse Act 1990

The Computer Misuse Act 1990 introduced three criminal offences: unauthorised access; unauthorised access with intent to commit a serious criminal offence; and unauthorised modification of computer material.

Any member of staff identifying or suspecting such activity must report it immediately.

The Data Protection Act

This covers personal data held on any form of electronic retrieval system (which can include CCTV and video recordings) and paper-based records.

Personal information is that information which can be identified with a living individual, either by name or indirectly. It can consist of anything from simply a name and address to the most sensitive information, such as medical or financial records.

If you use such data you must comply with the eight principles of the Act. They are, in simplified terms: -

1. Data must be processed fairly and lawfully.
2. Data must be obtained only for one or more specified and lawful processes and must not be further processed in any manner incompatible with that purpose or those purposes.
3. Data must be adequate, relevant and not excessive in relation to the purpose for which it is held.
4. Data shall be accurate and, where necessary, kept up-to-date.
5. Data shall not be kept longer than necessary for the purpose for which it is held.
6. Personal data shall be processed in accordance with the rights of data subjects.
7. Appropriate security measures must be taken against unauthorised or unlawful processing and against accidental loss or destruction of, or damage to, personal data.
8. Personal data must not be transferred to a country outside the EU unless that country provides an adequate level of data protection.

In practice this means that you need to be particularly careful about: -

1. The accuracy of data.
2. Deleting data. Part Two of this Guide requires departments to produce their own guidance on the retention and deletion of records. You should obtain a copy and comply with it.
3. Disposing of paper printouts that contain personal data. They must be shredded or put into a confidential waste bag.
4. Holding data on portable media, such as floppy discs, CDs or memory sticks. Such items must be secure at all times, and the data deleted from them as soon as it is no longer necessary.
5. Passing personal data to staff in other parts of the Academy, which would involve its use for purposes other than those for which it was given.
6. Passing personal data to other agencies. You must always seek advice and authorisation before doing this.
7. Leaving terminals unattended in a non-secure area when logged in to the network.
8. Designing forms to be used for collecting personal information.

Intellectual Property Rights

Staff must be aware of intellectual property rights, such as copyright, design rights and trade marks. Infringement can lead to legal action that may involve criminal proceedings.

This warning is particularly pertinent to the use of material available on the Internet. The same legal requirements apply.

Software Copyright
Users who buy software are responsible for ensuring that the software licence is held securely and available for verification.

Unauthorised Use of Equipment
The Academy's ICT equipment may not be used for unauthorised purposes. This could lead to criminal or fraudulent acts, waste valuable resources, or result in damage to hardware, software or data.

This includes playing computer games, except those supplied as a standard part of Microsoft Windows.

System Audits
The ICT Division gives notice that it will undertake electronic system audits to identify unauthorised, illegal or unlicensed software. These will not be obvious to users. Any such software is liable to immediate deletion.

Internal and external auditors may also undertake specific work to identify compliance by users.

8. Miscellaneous

Waste Disposal
Staff should take care when disposing of printouts that may contain any form of personal data. We encourage recycling of scrap paper, but this must not compromise confidential or personal information.

Floppy discs are now almost obsolete but require particular attention during disposal, since it is usually possible to recover deleted files. We therefore recommend that they are physically broken to prevent any further use.

Staff will be responsible for the destruction of their own personal floppy disks, as it may contain confidential data. ICT hardware, which needs to be disposed of, should be passed back to the ICT department for correct and safe disposal.

Accidental Verbal Disclosure of Information
Staff who have access to large databases should be aware of the risks of accidental verbal disclosure of information, and take measures to prevent it.
It is important not to disclose accidentally information of a personal nature, such as the name of an occupant at an address. Caution is required against people who may approach us in order to trace or harm someone. Staff should also be aware that accidentally disclosing information about the status of a person or an address can also compromise their security, and constitutes a breach of this Policy.