ICT Security Policy

POLICY AND PROCEDURE	**ICT Security Policy**
POLICY NUMBER	**ICT - 0002**
DATE OF FIRST ISSUE	**November 2014**
REISSUE DATE	**November 2018**
ISSUE NUMBER	**3**
APPROVING COMMITTEE	**EMT**
DATE OF APPROVAL	**October 2018**
RESPONSIBLE PERSON	**Director of Infrastructure**
EQUALITY IMPACT ASSESSMENT	**March 2015**
REVIEW DATE	**August 2019**

Document Number (if applicable)	Document Title

Contents

1. Purpose

The purpose of this Policy is to protect Ayrshire College's information assets and systems from all threats, whether internal or external, deliberate or accidental.

It is the policy of Ayrshire College to ensure that:

- Information will be protected against unauthorised access
- Confidentiality of information will be assured
- Integrity of information will be maintained
- Regulatory and legislative requirements will be met
- Business continuity plans will be produced, maintained and tested
- ICT security training will be available to all staff

2. Counter-Terrorism & Cyber Security

The policy also supports Section 26 of the Counter-Terrorism and Security Act 2015 (the Act) places a duty on certain bodies, listed in Schedule 6 to the Act, the *Prevent* strategy, published by the UK Government in 2011, is part of our overall counter-terrorism strategy, CONTEST. The aim of the *Prevent* strategy is to reduce the threat to the UK from terrorism by stopping people becoming terrorists or supporting terrorism.

Prevent Duty Guidance: for Scotland

https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/445978/3799_Revised_Prevent_Duty_Guidance__Scotland_V2.pdf

The ICT Security Policy also takes into consideration and will support the Government's National Cyber Security Policy. https://www.ncsc.gov.uk/

3. Policy Statement

Ayrshire College will ensure that it has transparent and robust processes in place to manage the key risks faced by the College in respect of ICT Security. The College understands that the regular review of risks faced and actions to manage and mitigate risk is a key responsibility of the Board of Management.

4. Equality Statement

The College is committed to providing equal opportunities to ensure its students, staff, customers and visitors are treated equally regardless of: gender reassignment; race, religion or belief; disability; age; marriage and civil partnerships; pregnancy and maternity; sexual orientation; sex.

5. Scope

The ICT Security Policy is intended for all College staff, companies or College partners who have an agreement in place which requires access to the College systems, Wi-Fi or network, Students using the College's ICT systems or data are covered by the College's 'Acceptable Use Policy' documents.

A separate Network Security Policy addresses all aspects of Network Security

The three main objectives of the ICT Security Policy are:

- To ensure that equipment, data, staff and agreed partners are adequately protected against any action that could adversely affect the College.
- To ensure that ICT Users are aware of and fully comply with all relevant legislation in this area.
- To create and maintain within the College a level of awareness of the need for ICT security to be an integral part of the day to day operation so that all staff understand the need for ICT security and their own responsibilities in this respect.

For the purposes of this document the terms ‘ICT’ (or ‘ICT system’), ‘ICT data’ and ‘ICT user’ are defined as follows:

- ‘ICT’ (or ‘ICT system’) means any device or combination of devices used for the storage or processing of data and includes: workstation (net book, notebook, desktop/tower PC), PDA, cash till, server or any other similar device.
- ‘ICT data’ means any information stored and processed within the ICT system and includes programs, text, pictures, sound, video and any form
- digital music. ‘ICT user’ applies to any College employee, student or other authorised person who uses the College ICT systems and/or data.

6. Responsibilities

The ICT Security Policy relies on management and ICT User actions to ensure that its aims are achieved. The roles and responsibilities are defined below.

Board of Management

The Board of Management through the Executive Management Team have the ultimate corporate responsibility for ensuring that the College complies with the legislative requirements relating to the use of ICT systems and for disseminating policy on ICT security and other ICT related matters.

Vice Principal-Corporate Services

The Vice Principal-Corporate Services through the Director of Infrastructure is responsible for ensuring that the legislative requirements relating to the use of ICT systems are met.

Director ICT

The Head of ICT is responsible for ensuring the College’s ICT Security Policy is adhered to and updated as required. The Director of Infrastructure is responsible for ensuring that the College fully complies with the Data Protection Act 1998.

The Director of Infrastructure is responsible for ensuring that the ICT Users of College systems and data are familiar with the relevant aspects of this Policy and that appropriate controls are in place. This is particularly important with the increased use of computers and laptops at home. Staff should exercise extreme care in the use of personal data at home to ensure legislation is not contravened and in particular the Data Protection Act 1998.

Head of ICT

The day to day responsibilities are delegated by the Head of ICT to the ICT Officer as nominated ICT Security Officer.

The Head of ICT is responsible for the College's ICT equipment, systems and data and will have direct control over these assets including the responsibility for controlling access to these assets and for defining and documenting the requisite level of protection.

The Head of ICT will administer the practical aspects of ICT protection and security including Ransomware, Malware and Cyber Security and to ensure that various functions are performed including maintaining the integrity of the data and producing the requisite back-up copies of data within procedures to mitigate the risk of any form of breach to the college ICT Security.

The Head of ICT is the nominated point of contact for ICT security issues and as such is responsible for notifying the Director of Infrastructure of any suspected or actual breach of ICT security occurring within the College.

The Director of Infrastructure should ensure that details of the suspected or actual breach are recorded and reported to the EMT. The Director of Infrastructure must advise EMT of any suspected or actual breach of ICT security pertaining to financial irregularity. The EMT through the Vice Principal-Corporate Systems shall thereafter notify any other relevant party e.g. Internal / External Auditor.

The Head of ICT will be fully conversant with the ICT Security Policy and maintain an up to date knowledge of best practice in this area.

ICT Technicians

The ICT Technicians will respond to actions delegated by the Head of ICT in order to ensure that the ICT System complies with the ICT Security Policy. The ICT Technicians will also monitor the College ICT System for breaches of security and inform the Head of ICT or the Director of Infrastructure.

Users

ICT Users are Staff, Students or authorised "guests" of the College who make use of the ICT system to support them in their work. All ICT Users of the College's ICT systems and data must comply with the requirements of this ICT Security Policy. The College has an Acceptable Use Policy which summarises the responsibilities of ICT Users.

ICT Users are responsible for notifying the Head of ICT of any suspected or actual breach of ICT security. In exceptional circumstances, ICT Users may report any such breach directly to the Director of Infrastructure or the Vice Principal-Corporate Systems.

ICT Users are responsible for the equipment they use including:

- Physical Security
- Security of Data
- Ransomware, Malware and Cyber Security
- Personal Passwords.

7. Procedures

Resources

Resources are allocated each year to ensure the security of the College's ICT systems and to enable ICT Users to comply fully with the legal requirements and policies covered in this policy. If insufficient resources are available to fully implement this policy then the potential risks must be documented and reported to EMT by the Director of Infrastructure.

Training

Suitable training for all ICT Users and documentation to promote the proper use of ICT systems will be provided. ICT Users will also be given adequate information on the policies, procedures and facilities to help safeguard these systems and related data.

In addition, ICT Users will be made aware of the value and importance of such ICT systems, data and the latest impact to ICT Security with regard to Malware, Ransomware and Cyber Security to ensure all college data of a financial, confidential or sensitive nature, and be made aware of their personal responsibilities for ICT security.

To help achieve these aims, the relevant parts of the ICT Security Policy and any other information on the use of particular facilities and techniques to protect the systems or data will be disseminated to ICT Users.

The Director of Infrastructure must ensure that adequate procedures are established in respect of the ICT security implications of personnel changes. Suitable measures should be applied that provide for continuity of ICT security.

These measures as a minimum must include:

- That new staff have been issued with and have read the appropriate documentation relating to ICT security;
- The access rights to systems granted to an individual ICT User and their limitations on the use of the data in relation to the data protection registrations in place;
- That those rights have been amended or withdrawn due to a change to responsibilities or staff leaving the College.

Physical Security

The College should ensure the physical security of rooms containing ICT equipment (including associated cabling). As far as practicable, only authorised persons should be admitted to rooms that contain servers or provide access to data. The server rooms should be locked when left unattended.

The Head of ICT must ensure appropriate arrangements are applied for the removal of any ICT equipment from its normal location. These arrangements should take into consideration the risks associated with the removal and the impact these risks might have.

Equipment Sighting

Reasonable care must be taken in the sighting of computer screens, keyboards, printers or other similar devices. Wherever possible, and depending upon the sensitivity of the data, ICT Users should observe the following precautions:

Devices are positioned in such a way that information stored or being processed cannot be viewed by persons not authorised to know the information;

Equipment is sighted to avoid environmental damage from causes such as dust & heat;

ICT Users should not leave computers logged-on when unattended if unauthorised access to the data held can be gained.

ICT Users should not leave hard copies of sensitive data unattended on desks. The same rules apply when accessing the College's ICT System or ICT data away from College, e.g. at an ICT User's home or visiting another College.

ICT Asset Management

The Director of Infrastructure shall comply with the College's Financial Regulations and Asset Management procedure.

Legitimate Use

The College's ICT facilities must not be used in any way that breaks the law or breaches College standards.

Such breaches include, but are not limited to:

- Making, distributing or using unlicensed software or data;
- Making or sending threatening, offensive, or harassing messages;
- Creating, possessing or distributing obscene material;
- Unauthorised personal use of the College's computer facilities.

Private Hardware & Software

Dangers can occur from the use of unlicensed software and/or software infected with a computer virus. It is vital that any private software is acquired from a responsible source and is used strictly in accordance with the terms of the licence. The use of all private hardware for College purposes must first be approved by the Head of ICT or the Director of Infrastructure in their absence.

ICT Security Facilities

In addition consideration should also be given to including appropriate processing controls such as audit trails, input validation checks, control totals for output, reports on attempted unauthorised access, etc.

For new systems, it is recommended that such facilities be confirmed at the time of installing the system. Information on the range of such facilities can be sought from the ICT Services Team.

Portable Computers & Hand Held Devices

ICT Users in the possession of a portable, laptop, notebook, palmtop and other transportable computers containing ‘secret’ or ‘confidential’ Ayrshire College information, should not leave these computers unattended at any time unless the information is stored in encrypted form.

To prevent unauthorised disclosure, ICT Users in the possession of transportable computers containing unencrypted ‘secret’ or ‘confidential’ Ayrshire College information must not check these computers in airline luggage systems, with hotel porters etc. These computers must remain in the possession of the traveller as hand luggage.

Whenever ‘secret’ or ‘confidential’ information is written to form of storage media, then the storage media must be suitably marked with the highest relevant sensitivity classification. When not in use, this media must be stored in locked safe, locked furniture or similarly secured location.

Encryption

As a minimum, all devices of the ICT System that are portable should be fully encrypted to meet the current encryption standard FIPS 140-2 (cryptographic modules, software and hardware) and FIPS – 197. Encryption products certified via CESG's CPA or CAPS schemes to at least FOUNDATION grade would also meet the current standard.

Devices subject to encryption may include:

- Laptops
- PDAs
- Smartphones
- USB Pen drives/Memory cards

Where technology prevents the use of encryption (e.g. SD Memory Cards used in Digital Cameras) then any data deemed sensitive or staff and student personal data should not be stored on these devices.

When using encryption systems that require a password to access the system, the same FIPS standards apply.

Data Backups

In order to ensure that essential services and facilities are restored as quickly as possible following an ICT system failure, back-up copies of stored data will be taken at regular intervals as determined by the Head of ICT. This is dependent upon the importance and quantity of the data concerned.

Where programs and data are held on the College's systems or other multi-ICT User system, data security and restoration is covered by Ayrshire College procedures.

Data essential for the day to day running and management of the College should be stored on the College's network. Backups containing data that must be protected and should be clearly marked in terms of time and data held. Backup media should be stored away from the system to which they relate in a restricted access fireproof location, preferably off site.

Instructions for re-installing data or files from backup should be fully documented and security copies should be regularly tested to ensure that they enable the systems/relevant file to be re-loaded in cases of system failure.

Operating System Patching

The Head of ICT will ensure that all machines defined as part of the ICT System are up to date by applying manufacturer's updates to the operating systems. A record should be maintained of all machines running operating systems that can be patched along with each machine's patch status.

Virus Protection

The College will use appropriate Anti-virus software for all College ICT systems.

All ICT Users should take precautions to avoid malicious software that may destroy or corrupt data.

Staff who have laptops which are taken away from College and may spend periods of days and/or weeks disconnected from the College's network, must take the necessary steps to ensure anti-virus protection software on their laptop is updated as soon as possible after a period of time off the network.

The College will ensure that every ICT User is aware that any device in the ICT system (PC, laptops, net book, PDA, iPad's or other mobile devices, cash tills) with a suspected or actual computer virus infection must be disconnected from the network and be reported immediately to the Head of ICT who must take appropriate action, which includes removing the source of infection.

Ayrshire College could be open to a legal action for negligence should a third party suffer "loss" as a consequence of a computer virus on College equipment.

The College's internet link is provided by JISC (which is procured through a 3rd party). The terms of this connection retain a sanction to remove the connection from the whole JANET MAN if significant viral activity is detected by that 3rd party provider.

The College will be notified by JANET if this is where the viral activity arises from. The Head of ICT is responsible for the treatment of any virus problems within an agreed period from notification by Clydenet or JANET. The network provider reserves the right to disconnect a College that fails to comply with a notification order to protect the access for all other Colleges.

Any third-party laptops not normally connected to the College network must be checked by the ICT Technicians for viruses and anti-virus software before being allowed to connect to the network (further details can be found in the network security policy).

The College will ensure that up-to-date anti-virus signatures are applied to all servers and that they are available for ICT Users to apply, or are automatically applied, to PCs or laptops.

Disposal of Waste ICT Media

Disposal of waste ICT media such as print-outs, floppy diskettes, DVD's, CDROM's, magnetic tapes and Memory Sticks will be made with regard to the sensitivity of the information they contain. For example, paper will be shredded if any confidential information from it could be derived.

The Data Protection Act requires that adequate mechanisms are used when disposing of media containing personal data.

Disposal of ICT Equipment

The Data Protection Act requires that any personal data held on a part of the ICT system subject to disposal be destroyed.

Prior to the transfer or disposal of any ICT equipment the ICT Service Leader must ensure that any personal data or software is removed from the machine.

Normal write-off/disposal rules as stated in the College Financial Regulations apply. Any ICT equipment must be disposed of in accordance with WEEE regulations.

It is important to ensure that any copies of the software remaining on a machine being relinquished are legitimate. Due care and attention should be taken to avoid infringing software and data copyright and licensing restrictions by supplying unlicensed copies of software inadvertently.

Repair of ICT Equipment

If a machine, or its permanent storage (usually a disk drive), is required to be repaired by a third party the significance of any data held must be considered. If data is particularly sensitive it must be removed from hard disks and stored on floppy disk or other media for subsequent reinstallation, if possible. The College will ensure that third parties are currently registered under the Data Protection Act as personnel authorised to see data and as such are bound by the same rules as College staff in relation to not divulging the data or making any unauthorised use of it.

ICT Security Incidents

All suspected or actual breaches of ICT security shall be reported to the Head of ICT or the Director of Infrastructure, who should ensure a speedy and effective response to be made to an ICT security incident, including securing useable evidence of breaches and evidence of any weakness in existing security arrangements. The Director of Infrastructure must also establish the operational or financial requirements to restore the ICT service quickly.

The Audit Commission's Survey of Computer Fraud and Abuse 1990 revealed that over 50% of incidents of ICT misuse are uncovered accidentally. It is important that ICT Users are given positive encouragement to be vigilant towards any suspicious event relating to ICT use.

It should be recognised that the College and its staff may be open to a legal action for negligence if a person or organisation suffers a "loss" as a consequence of a breach of ICT security within the College where insufficient action had been taken to resolve the breach.

Acceptable Use Policy

The College's Acceptable Use Policy applies to all College staff, students and third parties. The policy covers the use of email, the Internet, services accessed through the Internet and local file and network usage. The conditions of use are explained in the policy. For all Students, the College will ensure that the relevant 'Acceptable Use Policy' document is issued and their signature on the enrolment form is agreement that the student will comply with the 'Acceptable Use Policy'. In addition, copies of the 'Acceptable Use Policy' document and consent form will be issued to all visitors who will be using Ayrshire College ICT resources.

Personal Use

The College has devoted time and effort into developing the ICT Systems to assist staff in discharging their responsibilities. It is recognised that there are times when you may want to use the Systems for non-work related purposes.

The College permits you to use the Systems for personal use.

- You must not use the systems for personal use during working hours. You must not allow personal use of systems to interfere with your day to day duties. Any non-job related use of the systems during working hours may be subject to disciplinary action.
- You must not use College software for personal use unless the terms of the licence permit.
- Use of the systems should at all times be strictly in accordance with the provisions of the Personal Use statement above.
- You are responsible for any non business related file which is stored on your computer.
- When accessing the internet for non work purposes you may only view web pages and download PDF files.

Staff E-mail

Staff at Ayrshire College should remember that the e-mail account assigned to them is for business use only and should ensure that their college e-mail account is not used to express personal opinions including political comments.

Disciplinary Actions

Breaches of this Policy may result in disciplinary action up to and including dismissal. They may also result in you being prosecuted under the Computer Misuse Act 1990, and may lead to prosecution of the College and the individual(s) concerned and/or civil claims for damages.

7. Review

This Policy will be reviewed in April 2019.