

## Purpose of Policy

Malicious attacks on education networks can cause damage to equipment, loss of services, and grant unauthorised users access to financial and student data. It is important that a policy is in place to ensure that the college network infrastructure is secure from unauthorised entry and that servers are protected within this infrastructure.

This policy has three aims:

- To raise awareness of security issues and threats with staff and students
- Minimise risks to college network services and services from unauthorised or malicious entry.
- To comply with UKERNA and Janet requirements for primary connections

## Scope

This policy will cover the protection of College networks, networking devices, servers and software only. It does not apply to general physical security of equipment or offices (which should be a matter of course), neither does it apply to security of information held on these systems, which is covered by other related policies (see below).

## Policy

It is the responsibility of City College Coventry employees, contractors, vendors and agents with access privileges to City College Coventry's corporate network to ensure that they have read, understood and comply with the implementation of this policy and any other related policies as detailed below.

It is also the responsibility of the Technical Services Manager to ensure that the policy is correctly enforced and that any City College Coventry employees implementing IT systems follow the guidelines stated in this document.

Having been granted access to college systems, staff will comply with the requirements of the Data Protection Act 1998 when processing relevant data as per the College Data Protection Policy.

Breach of this policy is subject to the disciplinary procedures of the College.

## Contribution to Achievement of the College's Mission

The College's Mission is *'Responding to Diversity, Raising the Standard, Taking Education Further'*. This Policy contributes to the Mission by securing the standards of the College's Information Technology facilities.

## Implementation

- Computers cannot be brought in from employee's homes and connected to the College network.
- It is the duty of staff to act responsibly whilst using the college's network and internet connections. It is also the duty of staff to ensure that students use these facilities in a responsible and safe manner.
- It is the responsibility of both staff and students to comply with investigations into breaches of security.

- Access to the College network through the firewall will only be permitted for legitimate or support uses. Vendors requiring access for legitimate purposes must supply information such as protocol, source ip address, port number and reason for access.
- Any changes to firewall access control lists must be authorised by the network & security manger before implementation. All changes to configuration must be documented and back-ups taken of the active configuration to provide a rollback point.
- Must properly secure applications that require internet access as part of their functionality to protect against intrusion.

#### Monitoring and Impact Measurement

The effectiveness of this policy will be subject to ongoing monitoring by the Head of Technical Services, the Vice-Principal Strategy & Operations and subject to annual review by the executive Management Group. This policy will be developed/amended accordingly.

The content and effectiveness of this policy is also subject to scrutiny by Internal Audit and thus also considered by the Audit Committee of the Corporation.

The impact will be measured by the number of reported incidents of breach of security and the Internal Audit actions required to maintain a 'good' audit rating.

#### Related Documents

- Data Protection Policy
- Acceptable Use Rules
- Remote Access Rules

#### Definitions

Term	Definition
Protocol	A set of rules that control the communication between computers on a network.
IP address	The address through which, a computer access the network and internet
Port	The port that an application uses to talk to servers and other computers on the internet
Access-Control List	A list of ports and addresses that allow or deny the flow of information through a network

#### Publication of Policy

This policy will be made publicly available, provided to all members of staff via the Intranet and forwarded to appropriate bodies on request.

<b>Policy Review Date</b>	November 2010
<b>Executive member responsible for implementation</b>	Director of Estates

<b>Approval and Review History</b>
• Approved by the Corporation on 17th September 2003 (Minute C77/03)
• Reviewed and approved by the Corporation on 15th September 2004 (Minute C73/04)
• Reviewed and approved by the Corporation on 14th September 2005 (Minute C71/05)
• Reviewed and approved by the Corporation on 13th September 2006 (Minute C72/06)
• Reviewed and approved by the Corporation on 5th December 2007 (Minute C102/07)
• Reviewed and approved by the Principal (under delegated authority from the Corporation) at the Executive meeting of 13th July 2009 (Minute 4)

