



YMCA **Wales** Community College



Secure Systems Policy





Introduction

The YMCA Wales Community College (the College) prides itself on the effectiveness and efficiency of its security systems.

This document aims to layout the systems in place to ensure the continued security in relation to the following five areas:-

1. Buildings
2. Resources
3. Employees
4. Data
5. Finance

This policy is in addition to the MIS Security Policy.

1. Buildings

The College has ownership of one building, the headquarters offices in Llanishen, Cardiff. This building has a number of security systems: window and door locks, an alarm system, ground floor window bars and access by the public is restricted. The building has full insurance and annual fire safety checks. In addition, the building is located on a business park with on-site security personnel.

Checks are carried out to ensure that all venues where teaching is carried out have public liability insurance. A health and safety assessment is carried out by the Health & Safety Adviser and information is recorded and held at the headquarters office.

2. Resources

Where appropriate, capital equipment is covered by insurance, maintenance and servicing agreements.

All other resources are checked to ensure their safety before they are made available to learners or employees. All portable electronic equipment and headquarters computers are annually PAT tested.

At the beginning of any resource loan, all recipients sign to agree their responsibilities in ensuring the security of the equipment.

All written handouts, audio and video materials, where possible, contain copyright information.

3. Employees

All employees are CRB checked for their suitability to work within the education sector and hold relevant teaching qualifications and / or experience in their subject area. CRB checks are renewed every three years.

All employees are covered by the College's insurance policy for personal injury. At induction employees are made aware of basic security procedures for their own safety and that of the learners for whom they are responsible. Employees are also informed of security procedures with regard to data held on learners. See following section on Data Security.

4. Data

This section should be read in conjunction with the College's MIS Security Policy, MIS Data Protection Policy, MIS Data Security and Archive Policy and Information Systems Procedures Policy.

Access

All access to data is restricted. Paper-based sensitive personal and financial data is stored in locked filing cabinets, accessible only by authorised employees. Electronic data is stored on College systems, all of which are only accessible via passwords.

Some electronic data is accessible through the internal College network – see the Information Systems Procedures Policy – Network Security Section.

The College holds various types of data e.g. financial and personal data on employees and learners (both electronically and in paper form).

Learner Data

The number of employees who have access to data is controlled, i.e. members of the full-time employees team or the course tutor. Partner organisations may also retain information on learners, following their own security guidelines. All of the above personnel are made aware at induction of the importance of keeping learners' information secure.

Data is retained in paper format on student enrolment forms which are kept in a locked cabinet at the College's headquarters. Data is also stored electronically on the College's server. Access to this information is via password. The only organisations to whom data is passed are awarding bodies when accreditation is sought and the Welsh Assembly Government (WAG).

Tutors retain limited information on learners to enable them to work effectively. Such information is retained within the tutor's course file.

Employees

Data on employees is retained in paper format in a locked cabinet at the headquarters offices. Some data is stored electronically on the College's Database. Information on employees is only passed to WAG in an anonymous form.

Relevant personal and banking details are passed onto the external accountants in order to process the payroll and inform HMRC.

Financial

All paper-based financial information is stored in a locked filing cabinet, accessible only by the Finance Officer and Head of College. Electronic financial data is accessible only via password at a single workstation. Secure electronic backups and physical archives are created in accordance with the MIS Data Security and Archiving Policy.

5. Finance

College monies are held in six separate bank accounts. Access to monies is via two signatories, the Head of College and one of three other named signatories.

A limited amount of petty cash is available in a locked tin within a locked cabinet. Access to this money is only available with approval by the Finance Officer or the Head of College.

On-line banking is utilised through the bank-provided secure website. Access is via chip & pin cards issued to relevant signatories and two separate signatories are still required to authorise transactions on-line. See Information Systems Procedures Policy – Network Security Section.

Monitoring

The Head of College will assess the effectiveness and efficiency of its security systems by spot checks to ensure the above systems are in place and meet the security requirements of the College.

Identifying Risks

The College has identified a range of risks which are recorded in the Risk Register.

All risks have been graded and where possible control measures put in place to minimise those risks (see also, Risk Management Policy.)

Adopted March 2006

Amended May 2010

Review August 2011