



YMCA **Wales** Community College



Management Information Systems Policies





Contents

	Page
1. Introduction	3
2. Staff And Learner Access And Entitlement Policy	3
3. MIS Service Delivery Policy	4
4. Data Security And Archiving Policy	5
5. Internet And E-Mail Usage Policy	6
6. Security Policy	7
7. Disaster Recovery Policy	8
8. Data Protection Policy	9
9. Information Policy	10
10. Information Code Of Conduct For Learners	11
11. Information Code Of Conduct For Staff	12

Introduction

This document is a collection of policies relating to the Management Information Systems of YMCA Wales Community College ('the College').

These policies are in some part related to the Information Systems Procedures Policy and Secure Systems Policy and should be read in conjunction with them.

Staff and Learner Access and Entitlement Policy

All members of the College will have access to the information they require for their role within the College.

Access includes both the system permissions to be able to view and/or amend information as appropriate, and also access to appropriate physical resources to permit that access.

Information should be available for sharing, unless there are clear reasons to the contrary – e.g. Confidentiality.

All members of the College should clearly understand their entitlements and responsibilities. Entitlements are privileges which may be withdrawn if responsibilities are not undertaken.

All members of the College will have appropriate training to enable them to access both the systems and information they require for their role.

Guidelines

Members of the College include all staff (full-time, part-time and sub-contracted), learners and governors.

All College staff will have access and entitlement to the information they require to fulfil their role.

Teaching staff will have access to the learning materials appropriate for their course(s), full details of learners on those courses, details of resources available for them to use on those courses such as facilities in teaching accommodation, library resources, and any budgetary allocations for materials, etc.

Learners will have access and entitlement to the information required to fulfil their role. Learners will have access to the learning materials appropriate for their course(s), details of resources available for them to use on those courses such as facilities in teaching accommodation, library resources, any budgetary allocations for materials, etc. and any information, personal to them, which the College holds.

Governors will have access and entitlement to the information required to fulfil their role, i.e. management, curriculum and statistical information.

Guidance for learners with learning difficulties and/or disabilities can be sought from the College's Disability Statement.

Operational Statement

Members of the College will be made aware of the above policy, as necessary.

MIS Service Delivery Policy

The MIS Service will provide members of the College with managed access to comprehensive, reliable, relevant and up-to-date information.

The MIS Service will be monitored and developed over time to ensure that it continues to meet the needs of the College.

Members of the College will be able to make legitimate enquiries quickly, easily and directly.

Summary and meaningful management reports will be available which are both accurate and timely.

Legitimate external information demands will be met before required deadlines.

Only resources (software, journals, data-sets, etc) for which there is a valid licence will be used.

Guidelines

Services may include the provision of information (e.g. library resources, financial accounts), the provision, maintenance and replacement of hardware, software, network services, etc. These should follow the premise of being “fit for purpose”.

Monitoring of the MIS Service should be in relation to both the strategic developments within the College, and user identified needs.

Quality issues will include timeliness, accuracy, response times, replacement cycles, etc. These should be determined for the core activities of the MIS Service and monitored to assess the performance of the Service.

Operational Statement

Members of the College will be made aware of the above policy, as necessary.

Data Security and Archiving Policy

All processing of data will comply with the Data Protection Act and other relevant legislation.

Access to information will require authorisation and the use of passwords.

All information will be protected from unauthorised access via external network connections.

Regular backups will be made and retained in accordance with an established schedule i.e. weekly.

Archives, in whatever format, will be established to relieve current file stores of infrequently required materials and thereby facilitate easier identification and access to frequently used items.

Retention schedules will be established for all the different categories of information within the College and archives will be regularly purged to maintain these schedules.

The format of the archived material will be considered and version and system details noted where appropriate. It may be necessary to retain earlier versions of software, or in some cases, technology, to ensure that archives can be accessed.

Guidelines

Backups will be made of all data/information on a weekly basis, and stored both on-site (all data) and off-site (critical data only). Backups will be encrypted and password protected.

Access to College data is protected from external access through an electronic firewall.

Use of strong passwords for all access within the College is enforced.

All non-electronic data will be retained for a minimum of 7 years. On expiry, paper data will be shredded.

Data stored electronically will be retained for as long as storage capacity allows but not less than 7 years. If it is necessary to expire electronic data it will be permanently deleted.

Operational Statement

Members of the College will be made aware of the above policy, as necessary.

Internet and E-Mail Usage Policy

Members of the College will only access the internet and email to fulfil their role within the College.

All use of the JANET network must conform to the JANET Acceptable Use Policy (this is available at www.ja.net/documents/use.html). At this time, this only applies to incoming email through 'fenet.swan.ac.uk'.

No member of the College should deliberately access the network without authorisation.

No member of the College should disclose passwords or authorisations to other individuals either within or outside the College.

The network must not be used for any illegal purpose, including libel, contravention of the Data Protection Acts, the Copyright Acts and Computer Misuse Act 1990.

Unsolicited advertising, obscene or offensive material, or material of a menacing nature, or designed to misinform, must not be transmitted.

Material that is likely to be considered obscene or offensive, or that which is illegal, must not be accessed.

The College has the ability to monitor e-mail and internet usage and all members should be aware that their use is not private. However, monitoring will only take place where breaches of this policy are known or suspected.

Members of the College should conform to common conventions of "netiquette". ("Netiquette" includes avoiding sending unwanted, useless or uncalled for e-mails; avoiding sending rude, angry and defamatory e-mails; use telephone or face-to-face when quicker or more efficient; do not forward e-mails unnecessarily; only give high priority to very urgent messages.)

The network must not be used in such a way as to deny access to others, disrupt their work, violate their privacy, corrupt or destroy their data or to waste staff time or resources.

Guidelines

In this policy 'the network' is defined as any internal College Local Area Network (LAN) and the connection provided between the LAN and the Internet external to the College.

Operational Statement

Members of the College will be made aware of the above policy, as necessary.

Security Policy

The Security Policy applies to all College information and the systems and technologies that support it.

All information, including backups, will be protected from unauthorised access.

The level of confidentiality and access will be assessed for all types of information.

Integrity of information will be maintained.

All breaches, or suspected breaches, of security will be reported and investigated.

Physical security will be maintained for premises, technology and information.

All members of the College will take recommended steps to prevent infection by computer viruses or other malicious software. These will include :

- the regular use of virus scanning software;
- caution when receiving e-mails with attachments (i.e. if the source is not known and reliable do not open);
- use only of reputable suppliers and websites;
- security of disks, memory sticks, and CD/DVD-ROM; and
- use only of College software – e.g. do not copy software from home computers, or use demonstration software.

All suspected viruses must be reported immediately.

Software must only be installed by authorised College staff.

Security issues will be monitored on an ongoing basis.

Guidelines

All College computers will continue to operate up-to-date, centrally managed, Anti-virus software.

Unauthorised access will be maintained through use of strong passwords and network security measures, i.e. firewall, IP filtering, etc.

Operational Statement

Members of the College will be made aware of the above policy, as necessary.

Procedures will be assessed against the Risk Management Policy

Disaster Recovery Policy

Good security and operational procedures will be maintained to reduce the frequency and severity with which disaster strikes.

The impact of the loss of any information, application or technology will be assessed.

Simple loss or corruption of data due to error or machine malfunction will normally be recovered by restoration from a back-up.

Loss of computer equipment due to malfunction, damage or theft of parts will normally be recovered by repair and/or replacement of parts, followed by data recovered from back-up.

Recovery of total loss of computer equipment due to fire, flooding, theft or other damage will vary depending on the impact of the loss. This may require purchase of new equipment, use of alternative equipment (at least as a temporary measure), or where the information/application is critical to the running of the College, a copy of the application (both the data and software) will be backed up and stored off-site by a designated member of staff.

Back-up facilities, both of data and equipment, will be stored separately from the main facilities to ensure that both are not consumed by the same disaster.

Operational Statement

Members of the College will be made aware of the above policy, as necessary.

Data Protection Policy

The College is required by law to comply with the Data Protection Act, 1998. The College is committed to ensuring that every current employee and registered learner complies with this Act regarding the confidentiality of any personal data held by the College, in whatever medium. This act came into force on 1st March 2000. Anyone who deals with personal information is required to handle that information confidentially and sensitively. The Data Protection Act includes measures to ensure that information is processed fairly and seeks to protect individuals' rights to confidentiality.

The Data Protection Act 1984 only covered personal data held in electronic format. The updated 1998 Act also covers personal data held on manual paper files.

What is meant by personal data? Personal Data is defined as any details relating to a living, identifiable individual. Within the College this applies to a great many categories of people: past and present learners and members of staff; potential learners and job applicants, etc.

The College needs to keep certain information about its past, current and potential employees and learners to allow it to function effectively and monitor performance and achievements. The College also needs to process information so that it can recruit and pay staff, organise programmes and comply with legal obligations to funding bodies, government regulations and company legislation such as health and safety and equal opportunities. To comply with the law, information must be accurate, collected and used fairly, stored safely, surrounded by adequate security and not disclosed to any other person. Individuals have to be informed why information on them is being collected, who will be able to access it and to what purposes it will be put. The individual concerned must agree that he or she understands and gives permission for the declared processing to take place, or it must be necessary for the legitimate business of the College.

The College must meet its moral and legal responsibilities and comply with the Data Protection Principles (www.dataprotection.gov.uk)

Personal data will be obtained only for specified and lawful purposes and will not be further processed in any manner incompatible with those purposes.

Personal data will be processed fairly and lawfully.

Personal data will, where possible, be accurate and up to date.

Only authorised College staff will have access to individual's personal information.

Personal data will not be kept for longer than is necessary. Methods of destruction will take into account the level of confidentiality of the data.

The College will, upon written request, provide individuals with all the details that it holds on them.

Information Policy

Responsibilities will be assigned for particular information practices and for specific information assets.

The right information will be acquired from outside and generated inside the College to meet its needs.

All members of the College will have access to the information they need, at the right time and in the right format.

Those who process and provide information should understand the needs of those using it.

Information will be fully exploited to meet the College's needs and to enable it to meet future challenges.

All members of the College will have appropriate opportunities to gain the skills and knowledge they require to use information effectively.

Technological infrastructure will support the information needs of the College.

Information standards will be maintained to aid transfer of information between systems.

The information needs of the College will be continually monitored.

All provision and use of information will comply with the current relevant legislative requirements.

Users within the College will, where necessary, be made aware of relevant legislation including: Data Protection Act, Freedom of Information Act, Computer Misuse Act, Copyright, Designs and Patents Act, Copyright (Computer Programs) Regulations, Obscene Publications Act, Telecommunications Act.

Operational Statement

Members of the College will be made aware of the above policy, as necessary.

Information Code of Conduct for Learners

You Must:

- a) comply with all relevant laws and regulations
- b) comply with relevant instructions from staff
- c) maintain back-ups of your work
- d) follow common standards of “netiquette” (see Internet and Email Usage Policy)
- e) use virus checking software, and check all personal storage media (e.g. floppy disks, CDs, memory sticks, etc.) before use, and report any suspected viruses immediately

You Must Not:

- a) use the College computer equipment without authorisation
- b) create, send or forward any obscene, offensive, threatening, defamatory or deliberately misleading material, including e-mails, text or images.
- c) access any material that is likely to be considered obscene or offensive, or that which is illegal.
- d) deliberately prevent other users from carrying out authorised activities, for example either by destroying or corrupting their data, or by overloading the systems and thereby causing them not to gain access
- e) infringe the copyright of others, or licensing agreements
- f) create or introduce a “virus” or any form of malicious software
- g) disable any security software from running, e.g. anti-virus, anti-spam, anti-spyware, firewall software.
- h) send any unsolicited commercial or advertising material
- i) attempt to reconfigure college computers, place shortcuts/aliases, software or clip art onto any local hard disk without authorisation to do so
- j) use personal storage media (e.g. floppy disks, CDs, memory sticks, etc.) without authorisation to do so.
- k) waste information resources.

Information Code of Conduct for Employees

You Must:

- a) comply with all relevant laws and regulations, including the JANET Acceptable Use Policy (www.ja.net/documents/use.html)
- b) comply with relevant instructions from staff within their areas of responsibility
- c) maintain your own back-ups of your work not automatically backed-up.
- d) where applicable, check your e-mail and pigeon hole regularly
- e) follow common standards of “netiquette” (see Internet and Email Usage Policy)
- f) use virus checking software, check all personal storage media (e.g. floppy disks, CDs, memory sticks, etc.) before use and report any suspected viruses immediately
- g) where applicable, ensure that learners are aware of their responsibilities for the security and use of information
- h) ensure that you have copyright clearance for all learning and teaching materials
- i) maintain information for which you are responsible to ensure its fitness for purpose
- j) facilitate access to information for which you are responsible to authorised persons
- k) ensure the security of portable computer equipment in your possession

You Must Not:

- a) use the College's computer equipment without authorisation
- b) create, send or forward any obscene, offensive, threatening, defamatory or deliberately misleading materials, including e-mails, text or images.
- c) access any material that is likely to be considered obscene or offensive, or that which is illegal.
- d) deliberately prevent other users from carrying out authorised activities, for example either by destroying or corrupting their data, or by overloading the systems and thereby causing them not to gain access

- e) infringe the copyright of others, or licensing agreements
- f) create or introduce a “virus” or any form of malicious software
- g) disable any security software from running, e.g. anti-virus, anti-spam, anti-spyware, firewall software, unless authorised to do so
- h) send any unsolicited commercial or advertising material
- i) attempt to reconfigure college computers, place shortcuts/aliases, software or clip art onto any local hard disk or file server, unless authorised to do so
- j) use personal storage media (e.g. floppy disks, CDs, memory sticks, etc.) unless authorised to do so
- k) waste information resources
- l) leave computing facilities unsecured or vulnerable to attack/theft.
- m) disclose personal or confidential information to unauthorised third parties

*Adopted Jun 2006
Amended May 2010
Review Aug 2011*