Policy & Procedure	IT Password Policy
Policy Area	IT
Version Number	2
Approving Committee	SMT
Date of Approval	26 September 2017
Date of Equality Impact Assessment	03 August 2016
Date of Review	01 November 2019
Responsible Senior Manager	Director, IT

History of Amendments

Date	Version/Pages/Sections Affected	Summary of changes
26 September 2017	Cover Policy Statement Appendix A	Post only for responsible Senior Manager. Entered in full. Change to Duration of Student Passwords.

Policy Statement

It is an aim of the College to encourage the responsible use of Information Technology [IT] by and for all of its stakeholders. This policy is aimed at reducing the likelihood of any breach in security practices or regulations that could jeopardise the business or commercial reputation of the College.

The College recognises the significant benefits in making Information Technologies available to staff, students and other stakeholders and seeks to minimise barriers to access whilst ensuring that systems and users are adequately protected. The College is also aware that there are potential issues associated with IT use and that all users will therefore benefit from having the Colleges' guiding rules and principles set out in advance of use.

This policy describes the conditions and criteria for the creation and provision of user access credentials and associated security password requirements.

Procedures associated with observing the policy are contained within this policy document. Template documents associated with this policy are located in the Forms section of the Staff Intranet.

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.

Please note this document is available in other formats, to request another format please email info@wcs.ac.uk

Contents

1. Purpose 1

2. Scope 1

3. Access to Systems 1

4. Active Directory Accounts 1

5. Guiding Principles 2

6. Password Components 2

7. Password Application 2

8. Role Based Access 2

9. Stand Alone Systems 3

10. Distributed Administration 3

11. Systems Admin Access 3

12. Guidance for Users 4

APPENDIX A – IT Password Policy 5

Equality Impact Assessment 6

1. Purpose

This policy details the College's rules and guidelines for the creation, administration and day to day use of the user credentials, and specifically access, passwords for the computer software or hardware systems being operated and fully administered by the College.

2. Scope

This policy applies to all students, employees, Board members, contractors, supplier support personnel, visitors or others given authorised access to the systems and infrastructure provided by West College Scotland.

This policy covers all computer software systems, hardware systems, data communication systems and all other components connected to or associated with these systems, which include, but is not limited to, personal and laptop computers, printers, servers and storage arrays, software applications, databases, e-mail systems and intranet or Internet based resource or service.

3. Access to Systems

The college provides automatic access to its IT systems and resources to all current employees, Board members and enrolled students. Access is for individual use and appropriate to role. Systems access is controlled via the provision of individual user credentials and associated security password.

4. Active Directory Accounts

Upon engagement or enrolment, College users are set-up within the College's Active Directory [AD] Domain. This system provides for the creation and management of individualised log-on credentials. The user account consists of three parts;

- individualised user identification,
- associated security password, and
- refined permissions set.

The user identification part takes the form of the *firstname.lastname* for Staff and Board of Management accounts and uses the unique nine digit student reference for Student accounts. These identifiers then associate each user with a unique, individual account and associated resource set.

The security password part is configured by the user and must be kept secret. Password secrecy ensures that access under a given user account is available solely to the individual for whom it has been provided.

The refined permission set part defines and controls access to the configuration options, resources and services that College processes dictate an individual's role or responsibilities entitle them to.

5. Guiding Principles

To enable access to applications and systems beyond AD, the College's aim to is to operate on the principle of "*same sign-on*" via the reuse of an individual's Active Directory credentials.

The primary and preferred method of establishing credential re-use is via the Lightweight Directory Access Protocol [LDAP].

However the College recognises that it is not always possible to associate third party stand-alone systems access with the pre-existing AD credentials. Where this situation is encountered and user access to a system is controlled via the systems local user access database, then access controls -subject to any constraints of the system- comparable to those generated for AD must be established.

6. Password Components

Active Directory provides the College with the tools to enforce six essential password components. These are;

- length,
- complexity,
- change frequency or duration,
- forcing a change at first login,
- history of password used, and
- lock out after incorrect attempts.

7. Password Application

The College recognises that different policies are required for differing stakeholder circumstance and Appendix **A** records;

- the settings that are enforced within AD,
- the systems that reuse these credentials, and
- the systems that cannot be set-up for credential re-use along with the password policies in use within these systems.

8. Role Based Access

Within AD, permissible data access is governed by an understanding of an individual's role or function within the College. Permission sets are created relative to individual or group need and access control exercised accordingly.

The New Start request process for staff [IT01] supports the identification and implementation of individualised role based systems access.

9. Stand Alone Systems

The College recognises that not all systems allow for LDAP integration. This is particularly relevant to systems deployed prior to merger. Where this situation exists the College will use the guiding principles to ensure both password parameters and access permission control(s) are set at the most effective level possible, from within available selections.

Where new systems are being procured, the College will require the inclusion of the provision for LDAP integration within the new systems tender requirement.

10. Distributed Administration

Responsibility for all user administration within Active Directory sits within the IT Directorate. For other systems the administration of user identities and individual or group permissions sets may be undertaken by staff with a different Directorate or Department.

These Directorates or Departments are deemed as “system owners” and the table in Appendix **A** records the system owners for the College’s main user access applications and systems.

This policy document covers all College applications and systems irrespective of where the administrative role is performed.

11. Systems Admin Access

System owners identified in Appendix **A** are responsible for the administration of the ‘owned’ system. Where systems administration is the role or function being undertaken, individualised administrative access, following the policy above, must also apply.

For College staff requiring user and administrative access, separate individualised accounts should be created, each being used only as and where appropriate. For the systems administration account, College password and permission set policy, including where applicable the re-use of same sign-on credentials, must be followed.

Where default systems administration identities and password exist within vendor systems, usually identified at set-up or on initial configuration, these must not be used for day to day administration. Default systems admin passwords must be changed from the vendor standard. Ideally this would form part of the systems design and be undertaken as part of the initial configurations.

12. Guidance for Users

Individual user identities and associated security passwords, with governing controls, are essential with modern systems. This is to ensure that data access is secured, auditable and managed appropriate to need.

Below are some additional guidelines that users must consider;

- when creating passwords, it is best practice to ensure that a password consists of a mix of upper and lower case letters, numbers and keyboard symbols,
- to avoid making it possible to second-guess a password, best practice is to avoid forming password from dictionary words, family or pet names,
- passwords should be memorised, kept secret and never shared. *A genuine system administrator acting in good faith would never ask a user to reveal their password, either in person, via email or over the telephone, and*
- passwords should not be written down. Where it is necessary to record multiple passwords for later retrieval, a '*security wallet'* application can be used. This software must then be secured with a complex, secret, memorised password. *IT staff can advise on appropriate software selection for desktop or mobile devices.*

This is best practice advice. It is applicable for user accounts with both College administered systems or where access to on-line resource is being made available to a College user, to support the needs of their role or function, by a third party provider.

IT Password Policy - Appendix A

				Password Parameters					
Software	**Function**	**System Owner**	**User group**	**Length**	**Complexity**	**Duration**	**History**	**Incorrect Attempts**	**On First logon**
Active Directory	Domain Authentication	IT	Staff	8 characters	On	60 days	2	5	Force Change
Active Directory	Domain Authentication	IT	Student	8 characters	Off	365 days	2	5	Force Change
Active Directory	Domain Authentication	IT	Distance Learning	8 characters	Off	No expiration	2	5	No
Exchange	Email	IT	Staff	Same Sign ON					
Office 365	Storage	IT	Staff	Same Sign ON					
iTrent	People Manager	HR & OD	Staff	Same Sign ON					
iTrent	Employee Self Service	HR & OD	Staff	Same Sign ON					
SharePoint	Staff Intranet	T&I	Staff	Same Sign ON					
Office 365	Email | Office | Storage	IT	Student	Same Sign ON					
WordPress	Student Intranet	T&I	Student | Staff	Same Sign ON					
Moodle	Virtual Learning Environment	T&I	Student | Staff	Same Sign ON					
Access All Areas [AAA]	Attendance & Timetable Portal	T&I	Student	Same Sign ON					
Your Essential Skills [YES]	Essential Skills Portal	Essential Skills	Student	Same Sign ON					
UnitE	Student Records	MIS	Staff	*Up to 8 characters*	*On*	*No forced expiration*	*Not configurable*	*5*	*Required - not system*
STAR portal	Attendance, Timetabling & Reports	MIS	Staff	Reuse of UnitE credentials					
Symmetry	Finance	Finance	Staff	*6*	*No*	*60*	*1*	*Not configurable*	*Not enforceable*

1. Equality Impact Assessment

Name of Policy/Procedure/Decision:
IT Password Policy

Provide a brief summary of the aims of the Policy/Procedure/Decision and main activities:
This Policy aims to encourage the responsible use of IT. It is aimed at reducing the likelihood of any breach in security practices or regulations that could jeopardise the business or commercial reputation of the College. This policy describes the conditions and criteria for the creation and provision of user access credentials and associated security password requirements.

Assessed By:	Clare Fraser	**Date:**	3 August 2016

This stage establishes whether a policy, procedure or decision will have a differential impact <u>from an equality perspective</u> on people who share protected characteristics or whether it is "equality neutral" (i.e. have no effect either positive or negative).

The protected characteristics are: age, disability, gender reassignment, pregnancy or maternity, race, religion or belief, sex and sexual orientation.

1. Who will benefit from this (students/staff/stakeholders)? Is there likely to be a positive impact on people who share protected characteristics, and if so, how? <u>Or</u> is it clear at this stage that it will be equality "neutral"? i.e. will not have a differential impact on any equality group/s?
Ultimately, all students, staff and stakeholders should benefit from responsible use of IT. There is no indication that this Policy will affect people who share protected characteristics differentially. This Policy could therefore be described as being "equality neutral"

2. Is there likely to be an adverse impact on people who share protected characteristics? If so, who may be affected and why? Or is it clear at this stage that it will be equality "neutral"?

There is no indication or likelihood of this Policy having an adverse or negative impact on people who share protected characteristics. The policy is written in clear and plain English, and the password rules should be comprehensible to all. In the event that any users require additional assistance, this will be provided by the College.

3. What action will you take to ensure that you are monitoring the impact of this policy?

Any complaints about the implementation of this Policy will be monitored.