Aberdare Community School
Ysgol Gymunedol Aberdâr

User Accounts Policy

Date Adopted	21st September 2022
Signature of Headteacher	
Signature of Chair of Governors	
Date to be reviewed	September 2023

USER ACCOUNTS POLICY

Review

This policy has been approved by the Technical Management Team and any amendments to it require the team's approval.

- Last approval: N/A
- Last review: N/A
- Next review: TBA

Overview

The purpose of this policy is to describe the acceptable use of the School's policy regarding user accounts for computer and network access.

Statement of Authority, Scope and Responsibilities

Introduction

This statement intends to outline a standard framework applicable to all policies maintained by Aberdare Community School Computing Services covering the use of School owned or licensed IT facilities and computer systems.

Authority

All users of computing facilities are bound by general law, Computing Services' policies, School Regulations, together with any specific rules that the IT Manager may from time to time introduce which apply to specific IT and computing facilities.

Purpose

It is the purpose of all computing Services' policies to ensure a safe, reliable and fit for purpose computing and IT infrastucture which aligns with the School’s main functions, namely that of being a centre of learning, encompassing teaching, research and training.

Scope

All Computing Services' policies are intended to outline the rules of conduct for all members of the School who access computer equipment and network resources as outlined above. The policies apply to the use of any IT facilities including hardware, software and networks, provided by the School and is applicable to all members of the School including staff, students, contractors, consultants, visitors and any other authorised users who may be either physically on-campus or accessing from remote locations.

Only authorised users of the School computer systems are entitled to use computing facilities. All members of the School are entitled to use computing facilities at all times when the network is available. Such use is subject to compliance with the School Regulations, this and other related policies.

Responsibilities

Computer facilities must not be misused within or outside the School. Everyone is expected at all times to conduct themselves in a responsible manner and to be considerate of other users' needs. Every user of computer systems has a duty to ensure they practice appropriate and proper use and must understand their responsibilities in this regard.

Senior management of Computing Services will be responsible for ensuring heads of Faculties, Departments, Schools, Centres and Units are aware of all relevant Computing Services policies, their implications and the responsibilities of all users.

Computing Services are responsible for policies under their control. Within each Faculty, Department, School, Centre or Unit certain areas of IT and computer security will be delegated to local support. This will be with full cooperation and support from Computing Services.

Acceptable Use

Please refer to IT Acceptable Use policy (AUP) for general policy regarding the use of IT facilites at the School.

Access to computing facilities is via individual username and password which allows access to login to central computing services, make use of private filespace, run software, access and use email facilities, share and transfer files and gain access to the Internet and the Web.

Accounts are issued for individual use only. For security purposes, users may not share, loan or give away account or password information to any other person. User accounts are to be used only by the assigned user of the account for authorised purposes. Passwords should not be

shared, written down, emailed or published. Default passwords should be changed as soon as practically possible.

Attempting to obtain another user's account password is strictly prohibited. User are required to change their password if they have reason to believe their account has been compromised in any way. Users are required to take all necessary precautions to prevent unauthorized access to computing resources.

Users must be aware of and understand IT Acceptable Use Policy (AUP) before accepting and using an account.

Eligibility

There are three main categories of people who are eligible for computing facilities.

- All students who are fully registered on a course at the School.
- All staff who are employees of the School.
- Staff who are not School employees but who are required, by a particular department, to have access to computing facilities. This third category, known as 'non-payroll staff' for the purposes of this policy, is discussed further below.

Non-Payroll Staff

Non-payroll staff must be real individuals. Accounts are not issued to groups, committees, services or similar.

In normal circumstances they will be visiting staff who are funded from outside sources, but they could be anyone the department considers in need of computing facilities for School work.

The department takes full responsibility for these non-payroll staff records and the computer usage of the staff concerned. They must remove the records when the non-payroll staff person leaves or no longer requires computing facilities.

It is a pre-condition of enjoying the services that follow from registration as a non-payroll member of staff that date of birth is provided to the IT Manager who is setting up the Account Information. The purpose of this is to provide a mechanism by which data from different sources can be recognised as such. The date of birth will be treated as confidential and will not be displayed or used for any other purpose.

Collection of Accounts

All students will automatically receive computer accounts at or prior to enrollment.

All other eligible users can go to the IT Managers office and ask to be set up with computing facilities. If eligibility is confirmed a username and initial password will be assigned.

Temporary Accounts

The use of temporary accounts should be minimised. Temporary accounts are a support overhead for Computing Services. Members of the School requiring access to School's computing facilities should acquire permanent usernames and use these for the duration of their employment or registration.

It is recognised that temporary usernames are required under special circumstances: for example, to provide a service for short courses and community courses.

Computing Services are prepared to create pools of temporary usernames, for a specified period, on the basis that a named individual member of staff is completely responsible for them and the pools of temporary accounts are minimised.

Temporary accounts shall follow the usual username account naming procedures. Temporary staff and student username accounts will, therefore, be differentiated for the purposes of file space allocation, backup, and security.

Individuals holding a Temporary Username are subject to the same terms and conditions, Policies and Regulations as any other computer user at the School. All temporary accounts are full and complete accounts and offer access to the same computing facilities.

A named person for any Department, Faculty or Center shall be responsible for the management and administration of any temporary accounts in use. When an individual 'inherits' a temporary username, the password on that account should be reset and all files deleted by the named person.

Account Closure

User accounts are subject to closure in the following circumstances:-

- Staff leaving the School – the account is closed on or shortly after the date of leave. It is expected the individual will arrange for appropriate data held under their account to be made accessible to others for business continuity.

- Staff that change to a new role in the school and need continued access to their user account privileges between roles can have their accounts and privileges extended when formal notification is given by an appropriate Department Head or representative.
- Closed accounts may only be re-opened following a meeting with the IT Manager.
- Dismissal where only School involvement exists - the account is closed immediately. Data stored under their account can be released with appropriate liaison with Computing Services and appropriate line manager or Head of Department or to an official authority (under normal legal safeguards) if appropriate or required.
- Dismissal where external agencies, in particular the police, are involved - the account is closed immediately.
- Sudden death through "normal" circumstances - the account is disabled immediately. Data stored under their account can be released with appropriate liaison with Computing Services and appropriate line manager or Head of Department or to other individuals (e.g. next of kin) if appropriate or required.
- Death involving a subsequent investigation - the account is disabled immediately. Data stored under their account can be released with appropriate liaison with Computing Services and appropriate line manager or Head of Department or to other individuals (e.g. next of kin) or to an official authority (under normal legal safeguards) if appropriate or required.
- Leaving Students - accounts will be marked for closure at some point within the summer vacation period. The account will close after a grace period of (at least) 30 days.

In all cases data is archived and will be recoverable for a period of time if necessary.

Related Documentation

This policy strongly encourages all users to familiarise themselves with the requirements, conditions and responsibilities of other related internal and external policy and legislative material that will inform their use of the School's IT services. These related sources are:

- School Regulations
- IT Acceptable Use Policy