Aberdare Community School
Ysgol Gymunedol Aberdâr

User File store Policy

Date Adopted	27th September 2023
Signature of Headteacher	
Signature of Chair of Governors	
Date to be reviewed	September 2025

USER FILESTORE 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

This policy defines allocation and management, including back up and virus checking, of the general user filestores for home directories and email provided by Computing Services.

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.

Filestore Allocation

All users with valid accounts have access to the centrally managed campus file server and email server on which they will be allocated storage for their exclusive use.
All accounts have filestore usage limits (disk quotas) placed on them and these are enforced dynamically. Current quotas for newly registered users are documented elsewhere. Every effort is made to provide all users with the disk space as they require. However, the total amount of disk space will always be finite. Requests for additional space may be granted depending on the circumstances and should be requested via the usual channels.
Shared storage space, both for email and general file storage can also be allocated.

Backup and Restore

Definitons

A backup is the process of copying active files from online disk storage to a suitable source so that files may be restored to disk in the event of damage to or loss of data.

An archive is the process of moving inactive files from online disk storage to a suitable source, i.e. deleting the files from disk after copying them, in order to release online storage for re-use.

Please note - archives are only taken by computing services for account closures.

Regular Backups

All central user filestore is backed up on a daily basis. A combination of full and incremental backups are performed throughout the day and overnight with all data being dumped to a suitable source. Backups are managed and kept secure with off site storage being performed on a periodic basis.

In association and agreement with their administrators, other data is also backed up as part of various Service Level Agreements (SLAs) that may be held with departments or other third parties for servers which are housed in the Machine Room or being managed by Computing Services.

Data Retention

Maximum data retention using the procedures currently operated for central file backup is 4 weeks. It should be noted however, that this does not necessarily mean that you will be able to recover your files from any given day in the last 4 weeks. Computing Services operates a rotating backup model known as a Father, Son backup. In its simplest terms we keep daily backups for a maximum of 7 days and weekly backups for a maximum of 4 weeks. This means that whilst we can and do recover the majority of files from the backups, there remains a small possibility that files may not be recoverable in certain scenario's. For example, if you happen to create and then delete a particular file in between 2 monthly backup sets, we may not be able to recover it in this instance as it would not exist on either of the monthly backup sets we have available. Additionally, whilst it is extremely unlikely, there is also a very small risk that a required file on a particular backup may be found to be unrecoverable or unreadable due to a write error. This is extremely rare and unlikely to happen, but nevertheless needs to be highlighted as a possible risk. Data recovery from backups whilst largely reliable, cannot be 100% guaranteed to be successful.

Data Restore

Computing Services manage the day-to-day running of the backup and restore process.

Active files that are accidentally damaged or deleted can normally be restored by the user using the "Previous Versions" facility from within the Windows Operating System.

Virus Checking

Data stored on the central file server will be subject to periodic virus checking procedures. Files will be scanned for known virus signatures using an up to date virus scanning engine. Files that contain virus signatures recognised by the scanning engine will be disinfected or quarantined. Disinfections will always be tried first and, if unsuccessful, the file will be quarantined. Quarantined files will not be accessible by the user. Computing Services should be contacted for access to any files which have been quarantined.

Filestore Scans

Computing Services will run regular scans on user's filestores to maintain system integrity and to check on any network misuse.