Aberdare Community School
Ysgol Gymunedol Aberdâr

Email Policy

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

E-MAIL 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 email and related services, systems and facilities.
The Policy is maintained and regulated by ACSCS and is cross-referenced to, and by, a number of other School policies and regulations.
The Policy will be made available to users of the email and related services and facilities. There will also be periodic review of the Policy and, if necessary, amendment from time to time. This will be necessary with regard to the expected development of the system, the operational use of the system and generally recognised best practice.
Email services are provided by the school to support its primary role of education and research and associated functions related to this role. See who can have an account for details of categories of people who are eligible for access to computing facilities.

Statement of authority and scope

This policy is intended to detail the rules of conduct for all members (generally staff and students) of the Aberdare Community School who use email and related services. This Email Policy applies to the use, for the purpose of sending or receiving email messages and attachments, of any IT facilities, including hardware, software and networks, provided by the school. The Policy is applicable to all members of the school including staff, students and other authorised users of school IT facilities.
Only authorised users of the school computer systems are entitled to use email facilities. All members of the school who agree and abide by the school regulations, are entitled to use computing facilities and email systems at all times when the network is available.

The school complies with and adheres to all its current legal responsibilities including Data Protection, Electronic Communication, Regulation of Investigatory Powers (RIP), Human Rights, Computer Misuse, Copyright and Intellectual Property

Statement of responsibilities

Individual users are responsible for their own actions. The use of email facilities by individuals at the Aberdare Community School assumes and implies compliance with this policy, without exception, and those Acts, Policies and Regulations referenced below and enacted or authorised by the school or other regulatory bodies. Every user of email systems has a duty to ensure they practice appropriate and proper use and must understand their responsibilities in this regard.
IT Manager of the Computing Services will be responsible for ensuring everyone is aware of this policy.
Computing Services are responsible for providing and maintaining central email systems.
Computing Services is responsible for email policy as a whole.

Acceptable use

General

The school's main purpose in providing IT facilities for email is to support the teaching, learning, research and approved business activities of the school. IT facilities provided by the school for email should not be abused. An absolute definition of abuse is difficult to achieve but certainly includes (but is not necessarily limited to):

- Creation or transmission of material which brings the school into disrepute.
- Creation or transmission of material that is illegal.
- The transmission of unsolicited commercial or advertising material, chain letters, press releases or other junk-mail of any kind
- The unauthorised transmission to a third party of confidential material concerning the activities of the School.
- The transmission of material such that this infringes the copyright of another person, including intellectual property rights.
- Activities that unreasonably waste staff effort or networked resources, or activities that unreasonably serve to deny service to other users.
- Activities that corrupt or destroy other users' data or disrupt the work of other users.
- Unreasonable or excessive personal use. (See below).
- Creation or transmission of any offensive, obscene or indecent images, data or other material. (Other than for reasons specified are below).
- Creation or transmission of material which is designed or likely to cause annoyance, inconvenience or anxiety.

- Creation or transmission of material that is abusive or threatening to others, serves to harass or bully others, discriminates or encourages discrimination on racial or ethnic grounds, or on grounds of gender, sexual orientation, marital status, disability, political or religious beliefs.
- Creation or transmission of defamatory material or material that includes claims of a deceptive nature.
- Activities that violate the privacy of others or unfairly criticise, misrepresent others; this includes copying distribution to other individuals.
- Creation or transmission of anonymous messages or deliberately forging messages or email header information, (ie without clear identification of the sender) or for 'flaming'.
- The deliberate unauthorised access to services and facilities.
- The unauthorised provision of access to school services and facilities by third parties.

Personal use

The school permits the use of its IT facilities for email by students, staff and other authorised users for a reasonable level of personal use. An absolute definition of abuse is difficult to achieve but certainly includes (but is not necessarily limited to):

- A level of use that is not detrimental to the main purpose for which the facilities are provided. *Priority must be given to use of resources for the main purpose for which they are provided.*
- Not being of a commercial or profit-making nature, or for any other form of personal financial gain.
- Not be of a nature that competes with the school in business.
- Not be connected with any use or application that conflicts with an employee's obligations to the school as their employer.
- Not be against the school's rules, regulations, policies and procedures and in particular this email policy.

Research and related

It is recognised that, in the course of their work or research, individuals of the school may have a requirement to transmit or receive material that would normally be defined as offensive, obscene, indecent or similar. In the case of properly supervised or lawful research purposes it is acceptable to do so. If in doubt advice should be sought.

Quotas and limits

All users have access to the centrally-managed email server. All accounts have quota limits placed on them. All file partitions are backed up on a regular basis. Accounts that are removed will have their files archived in accordance with the Account Closure and User Accounts policies. Unless specifically requested no archiving takes place.
Users receive email notification when approaching their quota limit and are encouraged to follow guidance in this email to manage their account. The final email that is received which takes an individual

over their limit will always be delivered. Once over quota no further email can be delivered to an individual's inbox until they have reduced their storage below their limit. Email that fails to be delivered because a user is over quota is held in the local mail queues for four days and the system will retry periodically to deliver. After four days the email is returned to sender.
Some limits on the size of an email that can be received and transmitted.

Virus checking

Computer viruses, trojan horses and worms are collectively known as malware. One common method of distributing malware is via email. All email communication through the ACSCS email gateways is checked for malware. Checking strategies include: refusing messages containing executable attachments, scanning messages for known malware or a combination of both techniques. Please note that this is a separate procedure and not related to the virus scanning policy applied to the central fileserver.
Messages containing malware will be retained for up to a month for administrative reasons. The **sender** of such messages will be informed of the viral content of their email. A similar message will be sent to the administrator(s) of the email gateways.

Aliases and lists

All members of staff will be allocated email aliases based on their initials and surname. Email alias duplications are possible so it is sometimes not possible to offer the exact email alias to users. Specific email aliases can be requested for individual or group use if there is legitimate requirement. Email aliases will not be changed for arbitrary or trivial reasons and the final decision on whether a reason is valid lies with Computing Services.
Email lists can also be created. Generally individuals requesting a list will be responsible for the ownership and management of the list.

Automatic email forwarding

Automatic forwarding or redirection of email to other mail domains is possible. Computing Services absolve all responsibility for email forwarded off the campus network. It is the individual's responsibility to set forwarding up and make sure the forwarding address is correct and the email service being used is reputable and reliable. Users must exercise caution when automatically forwarding any email to an outside network and question the need to even do so. All our email services are accessible to authorised users from the Internet.
Automatic forwarding or redirection of email within the *aberdareschool.co.uk* mail domain is not allowed. Allowing other people to access email can be achieved directly by sharing email folders and mailboxes.

Logging

Traffic through the ACSCS email gateways is logged. Logs include details of the flow of email but **not** the email content. Transaction logs are kept online for up to a month. Backups of these logs are kept for up to 3 months. Logs are available to authorised systems personnel for diagnostic and accounting reasons.

Standards

Standards are adhered to wherever possible. The ACSCS email gateways will attempt to verify the source and destination of email before being passed on. The *postmaster* and *abuse*email addresses are implemented in accordance with RFC 2142.

Spam and junk mail

Spam can be defined as "the mass electronic distribution of unsolicited email to individual email accounts". Junk mail is usually a result of spamming. In reality spam and junk mail are regarded as interlinked problems. There are methods individuals can use to filter this email.

Remote access

Remote access to School IMAP email servers (for reading email) is possible via the Internet or via the school's dial-in Remote Access Server (RAS). Remote access to other POP3 or IMAP mailboxes off campus is permitted via secure methods only.
Access to remote SMTP servers for sending mail is not permitted and is blocked at the firewall. Access to the school's SMTP servers from off campus is permitted for encrypted and authenticated connection only.

Incident handling and Data Protection

The school will investigate complaints received from both internal and external sources, about any unacceptable use of email that involves Computing Services IT facilities. Computing Services, in conjunction with other departments as appropriate, will be responsible for the collation of information from a technical perspective. It should be noted that logs are only kept for limited periods of time so the prompt reporting of any incidents which require investigation is recommended.
Where there is evidence of an offence it will be investigated in accordance with the school's disciplinary procedures applicable to all members of the school. In such cases Computing Services will act immediately with the priority of preventing any possible continuation of the incident. That is, accounts may be closed or email may be blocked to prevent further damage or similar occurring.

Related documentation

- School Regulations
- Acceptable Use Policy
- Proper Use Guidelines
- Junk Mail
- Data Protection
- Electronic Communications Act 2000
- Regulation of Investigatory Powers Act 2000
- Human Rights Act 1998
- Computer Misuse Act 1990
- Confidential Information, e-mail and the Internet