Aberdare Community School
Ysgol Gymunedol Aberdâr

IT Acceptable Use Policy

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

IT ACCEPTABLE USE 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

Introduction

As a user of IT services of the school you have a right to use its computing services; that right places responsibilities on you as a user which are outlined below. If you misuse school computing facilities in a way that constitutes a breach or disregard of the following policy, consequences associate with that breach and you may be in breach of other school regulations.

Ignorance of this policy (or those that it directs you to), and the responsibilities it places on you, is not an excuse in any situation where it is assessed that you have breached the policy and its requirements.

- Students are directed to this policy during their registration each year and are required to acknowledge their agreed adherence to and compliance with the policy.
- Staff are advised of this policy during their induction and of the school's requirement for them to adhere to the conditions therein.

A specific policy governing the use of telephones, email and the internet by staff is available on the school's shared areas and on the school's website and should be read in conjunction with this IT Acceptable Use Policy.
For the purposes of this policy the term "***computing services***" refers to any IT resource made available to you, any of the network borne services, applications or software products that you are provided access to and the network/data transport infrastructure that you use to access any of the services (including access to the Internet). Students and staff who connect their own IT to the school's network and the services available are particularly reminded that such use requires compliance to this policy.

User Authorisation

The User Accounts policy provides details regarding eligibility for an ACS User Account.
Access to all systems and services is controlled by a central computing account and password.
Students are allocated their User ID and initial password automatically as part of their registration with the school.
New staff paid through payroll are similarly automatically set up with a User ID and initial password. The procedures for any other category of personnel wishing to use the school's computing facilities are described in the User Accounts policy.

- Issuance and continued use of your User Account is conditional on your compliance with this policy.
- **User ID's and passwords are not to be shared**. Those who use another person's user credentials and those who share such credentials with others will be in breach of this policy.
- Initial default passwords issued to any user must be changed immediately following notification of account set up. Passwords should be routinely changed (every 3 months is recommended) and should be changed immediately if the user believes or suspects that their account has been compromised.
- Users with access to significant sensitive data will be requested to change their password at least annually. Failure to change the password will ultimately lead to the account being locked. This follows recommendations from both external and internal auditors.
- Help and guidance in managing your account is provided on the ACS web site (Your Account section).

General Conditions

- Your use of the school's computing services must at all times comply with the law.
- Your use of the school's computing services must not interfere with any others' use of these facilities and services.
- You are not entitled to use a computer that you have not been authorised to use.
- You must not access any program or data which has not been specifically authorised for your use.
- You must not use or copy any data or program belonging to other users without their express and specific permission.
- You must not alter computer material belonging to another user without the users' permission.
- You must not use school computing services to harass, defame, libel, slander, intimidate, impersonate or otherwise abuse another person.

- You must not use school computing services for the creation, collection, storage, downloading or displaying of any offensive, obscene, indecent or menacing images, data or material capable of being resolved into such. (There may be certain legitimate exceptions for academic purposes which would require the fullest disclosure and special authorisations)
- You must not use the school's computing services to conduct any form of commercial activity without express permission.
- You must not use the school's computing services to disseminate mass (unsolicited) mailings.
- You must not install, use or distribute software for which you do not have a licence.
- In general, use of school "computing services" should be for your study, research, teaching or the administrative purposes of the school. Modest use of the facilities and services for personal use is accepted so long as such activity does not contravene the conditions of this policy.
- Use of "computing services" for commercial work may be governed by software licence constraints and users should verify that the intended use is permissible under the terms of those licences with their local IT Support Staff or with ACS. Users must familiarise themselves and comply with the School's Software Management Policy.

Internet Access

The school campus network connects to the Internet via the RCT networks. All hosts on the campus network have potential access to the Internet and must be registered with ACS so that they can be allocated correct network addresses and host names. Non registered hosts will be denied access to the Internet. Guidance and advice regarding this requirement is provided under the Host Connection and IP Address Allocation policies on the ACS web site.

Using External Web 2.0 Services

Web 2.0 services offer attractive and useful applications services (Blogs, wikis, office systems, social bookmarking and social networking) to mention but a few. Use of such services however must comply with this policy. Before using such services – or expecting others to do so – it would be sensible to appreciate the issues that pertain to them.

Pros

- They may offer ready access to the latest, flexible technology.

- The social aspects of many services are enhanced by very widespread usage – there is no point in the school attempting to replicate del.icio.us or Facebook.
- Registration, account creation and access is normally very quick and cheap if not free.
- They offer routes to research collaboration or to peer group interaction.

Cons

- It is easy to be tempted to produce, and submit, content to such sites that you might later regret.
- What content or comments you do submit becomes potentially available across the world.
- Such content may have a longer life span than you might have imagined and could be accessed by a wide audience, including potential employers.
- Although such sites are external to the University, the way in which you use them, or the content that you submit to them might still lead you into trouble with the University and its policies and regulations.

Always read and consider the terms and conditions for any service you register with and ensure that you understand the implications of the service conditions. Further details are available in the Computer Use Guidelines – the Route to Good IT Citizenship.

Remote Access

Remote access to the campus network is possible via the Internet, Virtual Private Network (VPN) or via direct dial to the school's dial-in Remote Access Server (RAS). Remote access from external networks or across the Internet must be made via secure methods only. Further information and guidance is available on the ACS web site (Remote Access Server and VPN). Connections via VPN or RAS are considered direct connections to the campus network. As such, using the VPN service, dialling into the RAS, or generally accessing services remotely, subjects the user to the same conditions, requirements and responsibilities of this policy.
All connection attempts are logged.

Monitoring and Logging

Activities regarding network transactions may be monitored and logged and kept for an appropriate amount of time. Logs are taken for reasons of security, diagnostic and account/audit reasons. Logs are available only to authorised systems personnel and kept for no longer than necessary and in line with current data protection guidelines.

Such records and information are sometimes required - under law - by external agencies and authorities. ACS will comply with such requests when formally submitted.

Breaches of This Policy

Incidents which are determined to be in contravention of this policy will be assessed for their severity. Investigating such incidents may require the collection and evaluation of user related activity and evidence.
It is not possible to provide an exhaustive list of potential ways in which a user may contravene this policy but in general such breaches will be categorised into one of three levels of severity and each level of breach will carry with it a possible range of sanctions, consequences and/or penalties.
The Computer Use Guidelines – the Route to Good IT Citizenship provide useful advice and considerations that should guide and inform your use of Aberdare Community School computing resources. This guidance should keep you safe and ensure that you do not breach this Acceptable Use Policy.

Minor Breach

This level of breach will attract a verbal warning which will be held recorded for 12 months. In general this category will relate to behaviour or misuse of computer facilities that can be characterised as disruptive or a nuisance. Examples of this level of non-compliance would include:

- Taking food and/or drink into IT facilities where they are forbidden.
- Playing computer games on school provided IT.
- Sending nuisance (non-offensive) email.
- Behaving in a disruptive manner.

Not all first offences will automatically be categorised at this level since some may be of a significance or impact that elevates them to one of the higher levels of severity.

Moderate Breach

This level of breach will attract more substantial sanctions and/or penalties. These include:

- Progress Leaders will be informed of the nature and consequence of the offence.

- Access to computing facilities and services may be withdrawn (account suspension) until further notice.

Examples of this level of non-compliance would include:

- Repeated minor breaches within the above detailed 12 month period.
- Unauthorised access through the use of another user's credentials (username and password) or using a computer in an unauthorised area.
- Assisting or encouraging unauthorised access.
- Sending abusive, harassing, offensive or intimidating email.
- Maligning, defaming, slandering or libeling another person.
- Misuse of software or software licence infringement.
- Copyright infringement.
- Interference with workstation or computer configuration.

Severe Breach

This level of breach will attract more stringent sanctions, penalties and consequences than those above, and access to computing facilities and services may be withdrawn (account suspension) until the disciplinary process and its outcomes have been concluded. Possible sanctions include:

- Notification to Head Teacher and SMT.
- Withdrawal of access to computing facilities and services.
- For the most serious cases, referral via the SMT under the formal disciplinary procedures.

Examples of this level of breach would include:

- Repeated moderate breaches.
- Theft, vandalism or willful damage of/to IT facilities, services and resources.
- Forging email. i.e. masquerading as another person.
- Loading, viewing, storing or distributing pornographic or other offensive material.
- Unauthorised copying, storage or distribution of software.
- Any action, whilst using school computing services and facilities deemed likely to bring the school into disrepute.
- Attempting unauthorised access to a remote system.
- Attempting to jeopardise, damage circumvent or destroy IT systems security at either the Aberdare Community School or at any other site.
- Attempting to modify, damage or destroy another authorised users data
- Disruption of network communication capability or integrity through denial of service attacks, port scanning, monitoring, packet spoofing or network flooding activities.

Process

An investigation will be carried out, in confidence, by the Technical Management Team under the direction of the IT Manager. For staff, that investigative report will be passed to the Head Teacher and SMT, to be considered within the school's disciplinary procedures. For students, if a verbal warning is appropriate, this will be given by the Technical Management Team. If the breach is more serious, the report will be passed to the IT Manager to be considered under the preliminary student disciplinary procedures.

Recommended Reading

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:

- Aberdare Community School Regulations
- Aberdare Community School IT Security Policy
- Aberdare Community School Email Policy
- ACS User Accounts Policy
- ACS Host Connection Policy
- ACS IP Address Policy
- ACS Computer Systems Monitoring & Scanning Policy
- ACS VPN Guidance
- ACS Remote Access Server Guidelines
- Use of Telephones, Email and the Internet by Staff (to be available shortly)

Several related laws and their relevance in a school context are succinctly described in the Web Publishing Legal Requirements. There is also considerable school guidance regarding Data Protection and Freedom of Information.