Aberdare Community School
Ysgol Gymunedol Aberdâr

IT Security Policy

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

IT SECURITY 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: 1 Sept 2022

Introduction

This policy defines a framework by which the Aberdare Community School's computer systems, assets, infrastructure and computing environment will be protected from threats whether internal, external, deliberate or accidental.

Key Principles

All central computer systems, environments and information contained within them will be protected against unauthorised access.

All use of the school's IT facilities will comply with the IT Acceptable Use Policy.

Information kept within these systems will be managed securely, to comply with relevant data protection laws and to satisfy the school's expectations that such assets will be managed in a professional, safe and dependable manner. (See Guidance and Advice at Conditions of Use - IT Information Security).
All members of the school are required to familiarise themselves with this policy, to adhere to it and comply with its requirements.

Leaders of Learning and line managers have a responsibility for ensuring the implementation of, adherence to and compliance with this policy throughout their areas of functional responsibility.
The integrity of all central computer systems, the confidentiality of any information contained within or accessible on or via these systems is the responsibility of Aberdare Community School Computing Services (ACSCS).

All regulatory and legislative requirements regarding computer security and IT based information confidentiality and integrity will be addressed by Aberdare Community School Computing Services (ACSCS).

All breaches of security will be reported to and initially investigated by ACSCS.

All users have a responsibility to report promptly (to ACSCS) any incidents which may have an IT security implication for the school.

The Computing Environment

Technical Management Team, maintains and operates a range of central computing servers, systems, core network switches, edge network switches, backup systems, and the overall network infrastructure interconnecting these systems.

The computing environment is defined as all central computing resources and network infrastructure managed and overseen by ACSCS and all computing devices that can physically connect to it, and have been authorised (See Guidance and Advice at Conditions of Use - Connection) to connect to this environment. All are covered by this policy, including computing hardware and software, any school related data residing on these machines or accessible from these machines within the campus network environment and any media such as CD-ROMs, DVD-ROMs, portable storage devices and backup tapes.
All temporary and permanent connections via the school network, casual laptop docking points, the Wireless network and the Virtual Private Network (VPN) are similarly subject to the conditions of this policy.

Computing resources not owned by the school may be connected to the school's network. However, all such resources must comply with school's Guidance governing the use of computing resources.
(See Guidance and Advice at Conditions of Use - Connection)
Computing Services reserves the right to monitor, log, collect and analyze the content of all transmissions on networks maintained by both Computing Services and individual departments and organisations at any time deemed necessary for performance, fault diagnostic and IT Acceptable Use Policy compliance purposes.

Physical Security

Computing Services provides secure machine room facilities with protected power arrangements and climate controlled environments. Although primarily for the provision of central computing and network facilities, individual departments and, if appropriate, individuals are encouraged to consult ACSCS where

they have local systems in less than comparable environments with a view to those systems being housed in ACSCS Machine Room environs.

Any computer equipment in general office environments should be secured behind locked doors or protected by user log-out and or password protected screensavers whenever it is left unattended; and outside of general office hours.

Desktop machines in public areas should contain a device or mechanism for securing and protecting the main components and contents of the computer from theft.

Any portable equipment (such as laptops, memory sticks, CDs, PDAs, iPads etc) should use a log-on or power-on password wherever possible. Any unattended portable equipment should be physically secure, for example locked in an office or a desk drawer. When being transported in a vehicle they should be hidden from view. Staff should avoid storing sensitive information on portable equipment whenever possible (see data security section, at 5. below).

Staff who store confidential information on school owned portable equipment must ensure that such data is thoroughly and securely cleansed from that equipment when they leave the school's employment. Staff should consult ACSCS personnel (IT Supporters) for assistance and guidance on appropriate cleansing techniques and tools.

Data Security

The school attaches great import to the secure management of the data it holds and generates and will hold staff accountable for any inappropriate mismanagement or loss of it.

The school holds a variety of sensitive data including personal information about students and staff. If you have been given access to this information, you are reminded of your responsibilities under data protection law.

The school provides secure and practical remote access to information and data held within its various systems environments and IT infrastructure. In most cases, gaining access to such data from an off campus point of electronic access will prove sufficient – and safe - for most needs and is the recommended general mode of remote use of such data and information.

Any copying – or original creation – of sensitive data and information onto any form of portable media transport device or mechanism (Memory Stick, CD, DVD, External Hard Drive, PDA, portable music player, Laptop, etc.) or its transportation beyond the secure environment it was intended to be used within (systems

environment, PC environment, campus, office etc) carries additional responsibilities for the individual undertaking such activity.

These responsibilities should be clarified by performing a risk analysis, which considers the following rules/principles:

Employee/Student (personal) data should never leave the campus. In this context "leave" implies its physical transport to an external, and insecure location. Remote access to such data through an individuals approved access levels and permissions is distinct and not intended to be included in the term "leave".

If it is a unique or master version of data/information that has not been safely copied to a secure electronic or physical location or environment within the School's Computing Environment (implying that its subsequent loss is irrecoverable) then a copy should be made and stored securely prior to its offsite transportation for use.

If, following such a risk analysis, an individual identifies an imperative to take sensitive data off campus (in any media form) they are not to do so without prior consultation with ACSCS who can offer a range of suitable encryption solutions for the data prior to its removal from campus. Failure to comply with this requirement will be considered a serious breach of this policy.

Loss or Theft of Confidential Information

All incidences of loss or theft of confidential information should be reported so that they may be investigated. A data or IT security incident relating to breaches of security and/or confidentiality could range from computer users sharing passwords to the loss or theft of confidential information either inside or outside the school.

A security incident is any event that has resulted or could result in:

The disclosure of confidential information to any unauthorised person.
The integrity of the system or data being put at risk.
The availability of the system or information being put at risk.

Adverse impact, eg:

Negative impact on the reputation of the school.
Threat to personal safety or privacy.
Legal obligation or penalty.
Financial loss or disruption of activities.

The following is a list of examples of breaches of security and breaches of confidentiality. It is neither exclusive nor exhaustive and should be used as a guide only. If there is any doubt as to what constitutes an incident, it is better to inform your line manager who will then decide whether a report should be made.
Examples of breach of security:

Loss of computer equipment due to crime of carelessness.
Loss of portable media devices, eg – memory sticks etc.
Accessing any part of a database using someone else's password.
Finding doors and/or windows broken and/or forced entry gained to a secure room/building in which computer equipment exists.

Examples of a breach of confidentiality:

Finding confidential/personal information either in hard copy or on a portable media device outside School premises or in any of the School's common areas.
Finding any records about a staff member, student, or applicant in any location outside the School's premises.
Passing information to unauthorised people either verbally, written or electronically.

Specific Systems

Computer and network systems access is only via individual user accounts. See Guidance and Advice at Conditions of Use - User Accounts for further details and account eligibility.

Email

Email is not a completely secure medium. You should be conscious of this and consider how emails might be used by others. Remember that emails can easily be taken out of context, that once an email is sent you cannot control what the recipients might do with it, and that it is very easy to forward large amounts of information.
Similarly you should not necessarily trust what you receive in an email - in particular, you must never respond to an email request to give a username or password.
See the Electronic Communications Guidelines for further advice.

File Storage

All users have access to the centrally managed file storage. Use of the file storage is governed by the Guidance and Advice at Conditions of Use - User Filestore.
For the vast majority of applications the security of files stored centrally is appropriate. In particular this means they will be backed up. However if your files require a higher level of security, please contact Computing Services.

The Web

Users should consider the security implications of any information they put on the school's web-site, and the school reserves the right to remove any material which it deems inappropriate, illegal or offensive.
Users should not in any way use any areas of the school's web site for commercial purposes.
Users shall not in any way use web space to publish material which undermines IT security at the school. In particular this covers making information available about how IT security is implemented at a practical level, or any known weaknesses.

Campus Network

Individuals must seek permission from computing services representatives before connecting any machine to the LAN. Authorised connections will comply with the Guidance and Advice at Conditions of Use - Connection and IP Address Allocation. Computing Services may disconnect any unauthorised host from the network without warning.

Remote Access to Systems

Remote access is defined as accessing systems from a physically separate network. This may include:

Connections direct across the Internet

VPN Connections

Any user with a valid Aberdare Community School computer account may access systems as appropriate. Remote access is allowed via secure methods only. Remote connections to any campus IT services are subject to the same rules and regulations, policies and practices just as if they were physically on the campus. Computing Services shall provide the only VPN that may be used.
All connections via these services will be logged. No other remote access service shall be installed or set up, including single modems connected to servers or workstations. Any active dial-in services found to be in existence will be removed from the network.

Anti-Virus Security

Computing Services will provide means by which all users can download and install current versions of site-licensed virus protection software.

Users must ensure that they are running with adequate and up-to-date anti-virus software at all times. If any user suspects viral infection on their machine, a complete virus scan should be performed. If Computing Services detect a machine behaving abnormally due to a possible viral infection it will be disconnected from the network until deemed safe. Reconnection will usually only be after liaison with computing services.

Related Documentation

- School Regulations
- Acceptable Use Policy
- General Guidelines