Aberdare Community School
Ysgol Gymunedol Aberdâr

Computer Systems Monitoring and Scanning Policy

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

COMPUTER SYSTEMS MONITORING AND SCANNING 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 describes the Aberdare Community School's Computer Systems Monitoring and Scanning policy. The policy describes:

- The monitoring and scanning procedures approved by the school for this purpose.
- The prescribed circumstances which may be invoked to initiate the monitoring procedures.
- The procedures that shall ensure the execution of this monitoring policy conforms to the prescribed initiation circumstances, alone, and may be reviewed, ad hoc, by those with authority to intercept to prevent the abuse of the monitoring process.

The School may monitor and record communications:

- To collect evidence pertaining to compliance with this policy, and other related policies, regarding the acceptable use of computing facilities at the School.
- In the interests of national security, as required by Law.
- To prevent or detect crime, as by required by Law.
- To investigate or detect unauthorised use of the computing and network facilities of the School: as described in the School Regulations.
- To secure, fix, enhance or as an inherent part of effective and responsible systems operation.

The School may monitor but not record:

- Any communications to determine whether they are business or personal communications.

The School may scan systems:

- To investigate or detect unauthorised use of the computing and network facilities of the School: as described in the University Regulations.
- When a host or workstation is suspected of showing unauthorised or unusual activity on the network.
- In an effort to resolve a service problem, as a part of normal system operations and maintenance or to enhance the security of the overall campus network.
- To monitor compliance with School or Computing Services policy, to perform security assessments or to investigate security incidents.

Notice of Intent

The School hereby notifies all users of its Computing Services that it reserves the right to monitor all communications on those facilities in accordance with this policy. As such, authorised users of the system should be aware that personal communications, as well as communications relating to the functioning of the School made via the School's computing facilities, may be intercepted and/or monitored by Computing Services staff or other technical staff as specified in this policy.

Scope

The School has the right, at any time, to inspect all data held on the School's computer equipment, and to inspect all email and other electronic data entering, leaving, or within the School network to ensure conformity with:

- The School's regulations, policies and practices,
- Contractual agreements with third parties, and
- Telecommunications Regulations 2000

The School is obliged by law to report to the police the discovery of certain types of electronic data if that data is found on the School's computer systems or transmitted across the School's networks.

Many types of routine computer service tasks will involve members of Computing Services and other member of the School's technical staff having access to various levels of staff and student held data.

Examples include, but are not limited to:

- Email postmasters receiving mail failure notifications will often be sent the text of the failed message by the email server which has rejected or redirected the mail.
- Staff making or retrieving backup copies of data from file servers will, as part of the backup process, often be able to read the names of files held in staff and student accounts.
- Staff sorting output from shared printers prior to its dissemination to users will be able to view the content of that output.

Operational Practice

It is the Schools policy that the staff in Computing Services and in other administrative and academic units, may access staff and student data held on the School's computer systems, or inspect the content of email and other

electronic data entering, leaving or within the School's network. Attempts by any other member of staff to implement any such system of monitoring will be in breach of this policy and may be the subject of disciplinary proceedings.

The School recognises that, due to the nature of computer systems, data held on its systems, passing across its network, or printed out on the School's equipment, whether deliberately or accidentally, may be, at times, visible in human readable form. In such circumstances that data may well be viewed by the people other than the Computing Services or by relevant people in other administrative and academic departments. Such incidental viewing will not constitute a breach of this policy even where such viewing leads to the implementation of authorised monitoring and/or to the disciplinary procedures against the individual concerned.

The School reserves the right to monitor and access data held on its computer systems, email and other electronic data entering, leaving or within the School's network in the following circumstances:

Where by carrying out routine computing service tasks members of Computing Services and other members of the School technical staff discover data which breaches the Schools regulations, the School's contractual obligation to third parties, or UK law, or where the nature of the data suggests such a breach has occurred or will occur.

Where complaints are received by the authorities (such as the Police or UKERNA) suggesting that the School's computer systems or networks are being used to store, transmit or transfer data which breaches the School's regulations or the School's contractual obligation to their parties or UK law.

Where the School has been requested or required to monitor data by the police as part of a criminal investigation.

Where there is other reasonable suspicion that users are storing, transmitting or transferring data which breaches the School's regulations, the School's contractual obligation to their parties or UK law.

The School reserves the right to monitor the nature and extent of data uploaded and downloaded from the Internet. This may be carried out by various means including random filename searches of fileservers, email servers, cache servers etc. and real time logging of packet data as it traverses the School's gateway router.

Authority to Intercept

Specific monitoring of user data and specific access to user data by Computing Services staff may only be legitimately carried out under this policy. Additionally at least one of the following may be notified:

- The IT Manager.
- Schools SLT.

Specific monitoring of, or specific access to, user data should only take place for such time as is required to ascertain whether the user or users concerned are storing, transmitting or transferring data which breaches the

School's Regulations, the School's contractual obligations to third parties or UK Law. Long-term monitoring should only be permitted when this is specifically requested by the police as part of an on-going criminal investigation, or as part of an on-going internal investigation.

All specific monitoring or specific access to user data must be reported, along with the reasons for that action being taken and the result, if any, as soon as the monitoring is completed.

Data collected via specific monitoring of, or specific access to, user data shall (if not falling under a statutory exemption) be disclosable as part of a request for access under the Data Protection Act 1998. Data collected in this way will only be used, for example, for carrying out and concluding the investigation and any subsequent disciplinary proceedings and retained for at least 6 years afterwards.

Related Documentation

Legislation:

- RIP Act 2001
- The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000

Guidance:

- RIPA 2000: Home Office Guidelines