Ysgol Aberconwy

Information Security Policy

POLICY DOCUMENT NO: 76	ISSUE NO: 1

THIS POLICY HAS BEEN APPROVED BY THE FULL GOVERNING BODY

Signed:

Date: 02/07/24

Review due date : 01/07/26 LT Link : KB

Information Security Policy

Summary

What is this policy about?
The purpose of information security for the School is to protect all information held by the School, regardless of the format. This will help to safeguard the reputation of the School, to help the management of risk and to minimise the impact of information security incidents. Implementation of this policy will provide assurance to stakeholders, partners and the public that their information is held securely and used appropriately by the School, whilst complying with the relevant legislation.

Who is this policy for?
This policy relates to all information held by the school in any form, including personal data and will apply to all Employees, Governors and partner organisations who handle/access School information. This policy also applies to any contractual third parties and agents of the School who access the School's IT systems and IT equipment.

How does the School check this Policy is followed?
All staff and governors must complete a mandatory online module on information management to evidence that they understand data protection legislation. Should an incident occur, it would be investigated and appropriate action taken.

Who can you contact if you have questions about this policy?
The Head Teacher or the Business Manager

1 Introduction

Information security is not an option. Everyone is required to maintain a minimum level of information security. A breach of security during processing, storage or transfer of information could result in:

- financial loss
- personal injury to a member of staff, parent or pupil
- serious inconvenience
- embarrassment
- reputational damage
- legal proceedings against the School and possibly the individuals involved.

Non-compliance with this policy will be dealt with under the relevant School procedures and may result in disciplinary action, termination of contract, or criminal prosecution in the most serious of cases.
This policy should be read alongside the School's Data Protection Policy.

2 Objectives

The objective of this Information Security Policy is to ensure:

- Confidentiality - Information is only available to those that are authorised to gain access.
- Integrity - Safeguarding the accuracy and completeness of information and processing methods.
- Availability - Assurance that authorised users have access to information and associated assets when required.
- Risk management - Business damage and interruption caused by security incidents is minimised.
- Compliance - All legislative and regulatory requirements on the School are met.

This document provides the standard for Information Security developed by Ysgol Aberconwy. The highest standards of information security should be maintained across the School at all times.

3 Information format

This policy covers all formats of information, such as:

- Electronic, including e-mail and web sites
- Printed
- Handwritten
- Video
- Audio (including speech)
- Photographs / images

4 Responsibilities

It is the responsibility of all employees and elected Governors regardless of their seniority or position within the School to ensure that they conduct the business of the School in accordance with this Policy. This includes agency workers and third party organisations acting on behalf of the School.

Anyone who accesses School information that is not routinely made available to the public, and anyone that accesses the School IT Systems must:

a) Familiarise themselves with this Policy, and all applicable supporting policies, procedures, standards and guidelines. A summary of such associated documentation and appropriate legislation can be found in Appendix A.
b) Undertake approved Protecting Information training if available.

c) Only access systems and information, including reports and paper documents, to which they are authorised.
d) Use systems and information only for the purposes for which they have been authorised, and only from School controlled or authorised secure equipment and approved software.
e) Not disclose confidential, personal or sensitive information to any unauthorised person/s.
f) Ensure that confidential, personal or sensitive information is saved and sent using secure means.
g) Ensure that all passwords comply with the IT Security Policy. Keep passwords and other access credentials secure, and do not allow anyone else to use your account, equipment or media in your care to gain access to any IT system or other information asset.
h) Notify their immediate supervisor of any actual or suspected information security incident as soon as possible and also report it to the DPO by completing a data security incident form.
i) Never leave computers logged into the network unattended without locking the screen.
j) See IT Security Policy
k) Keep your desk clear of all confidential, personal or sensitive paper files and documents when you are not working on them. Maintain a clear desk policy when leaving your desk unattended for any period of time and out of office hours. Keep all confidential, personal or sensitive paper files and documents in secure, lockable cabinets.
l) Not routinely take confidential, personal or sensitive documents or materials home. Where this is unavoidable due to work requirements, do consider the use of lockable bags or cases when it is necessary to carry paper files or documents in person and also ensure that they are kept securely whilst in the home.
m) Confidential information must not be emailed to personal email accounts at home.
n) Ensure that documents containing confidential, personal or sensitive information sent to fax machines/printers (MFDs) are retrieved immediately so that unauthorised individuals have no opportunity to see the information.
o) Documents must be disposed of immediately once the requirement to dispose has been identified.
p) Not use any mobile device to store/transfer School information unless that device is encrypted.
q) Purchase all new laptops, mobile phones and devices capable of storing data, through IT to allow encryption software to be installed prior to being released.
r) All laptops, ipads and mobile devices must be locked away in a secure cabinet when not in use in the office or in the home and never left unattended in an unsecure location. Laptops may be secured to desks via suitable security cable.

Compliance with this Policy is mandatory, and any employee (including Governors) failing to comply could be subject to disciplinary procedures. The School monitors the content and usage of its systems and communications to check for policy compliance.

5 Management responsibilities

The Headteacher is responsible for:

a) Ensuring that the Information Security Policy is communicated and implemented within the school
b) Ensuring that any issues affecting information security, such as resourcing or funding are identified in a timely manner.
c) Promoting awareness of any relevant security awareness training, including induction training and e-learning.
d) Ensuring that system administrators receive prompt notification of employee role changes and departures.

6 Security Classification

Whatever form the information may take, or means by which it is shared, stored or processed, it should always be appropriately classified and handled according to that classification.
The School has two types of security classification:

- Non Sensitive - does not contain confidential, personal or sensitive information
- OFFICIAL - Sensitive – contains confidential, personal or sensitive information

7 IT systems

IT systems and the information they process and store are a vital asset to the School. In order to ensure the confidentiality, integrity and availability of these systems, an appropriate level of security must be achieved and maintained. The level of security implemented on each of the various IT systems will be consistent with the designated security classification of the information and the environment in which it operates.
Please refer to the IT Security Policy

8 Information Security Incidents

An information security incident can occur for a number of reasons, such as:

- Loss or theft of information or equipment on which information is stored.
- Inappropriate access controls allowing unauthorised use.
- Equipment failure.
- Human error.
- Unforeseen circumstances such as a fire or flood.
- Hacking /cyber-attack.
- 'Blagging' offences where information is obtained by someone deceiving the service/section who holds the information.

It is imperative that all known or suspected incidents are reported via the Head Teacher, Chair of Governors and DPO and investigated without delay. Time is crucial in minimising the risk to all parties and the immediate actions taken can often prevent an incident turning into something more serious. Please refer to the incident reporting procedure.

The priority in any incident response is **Containment and Recovery**. In all cases you should:

1. Establish the facts of the incident.
2. Identify the type of information involved - How sensitive or harmful is it? Are there protections in place such as encryption?
3. Establish who needs to be made aware of the incident and inform them of what they are expected to do to assist in the containment exercise.
4. Establish whether there is anything you can do to recover all or any of the information which can prevent or limit the damage the incident can cause. For example, it might be recovered by someone collecting the information straight away (if possible/practicable), or asking for it to be posted back or deleted.

It is expected that all incidents will be followed up with a thorough evaluation that:

- Identifies any weak points in the existing procedures and corrects as necessary.
- Raises staff awareness of information security issues, identifying and fulfilling any training requirement.