



# GP39 – DATA PROTECTION POLICY



<b>Last Review Date</b>	June 2024	<b>Next Review Date</b>	November 2024
<b>Leader of Policy Review</b>	Headteacher		
<b>Associated Policies</b>	FOI, RETENTION POLICY		

The Alun School's appointed Data Protection Officer is:

E2E Education  
The Annexe, Viscount House  
River Lane  
Saltney, Chester  
CH4 8RH  
dpo@e2e-education.co.uk  
01244 261379

## What is Information Governance?

Information Governance can mean different things to different people. It is a term that is used to describe the way we manage our obligations to the following legislation:

- GDPR
- Regulation of Investigatory Powers 2000
- Environmental Information Regulations 2004
- Freedom of Information Act 2000
- Re-use of Public Sector Information Regulations 2005
- Records Management (cop s46 FOIA)

It allows both the Alun School and its employees to ensure that both business and personal information is dealt with legally, securely, efficiently and effectively, in order to deliver the best possible services.

The Information Governance Framework sets out the way the Alun School handles information, in particular, the personal and sensitive data relating to our students, staff and suppliers.

## Information Governance - aims

The aims of Information Governance are to:

- comply with all relevant legislative requirements thereby protecting individuals, and organisation
- manage the creation, storage, movement and sharing of data in a secure and efficient manner

- support the provision of high quality service delivery by promoting the effective and appropriate use of information
- encourage staff and partners to work together, preventing duplication of information, effort and enabling more efficient use of shared data resources
- develop support arrangements which provide staff with information and appropriate Information Governance policies and guidance
- provide training and support to enable staff to discharge their responsibilities under the various acts - all to consistently high standards

The Alun School has a set of high level corporate policies in place which direct all Information Governance & Management. These are supported by detailed procedures setting out exactly how staff must work to follow our policy.

### **Information Risk Management**

Information risk is inherent in all administrative and business activities and everyone working for or on behalf of the authority continuously manages information risk.

Information risk management is an essential element of information governance and is an integral part of good management practice. The intent is to embed information risk management in a very practical way into business processes and functions.

### **Information Assets**

An information asset is a body of information, defined and managed as a single unit so it can be understood, shared, protected and exploited effectively. Information Assets (IA) have recognisable and manageable value, information lifecycle. By identifying IAs it is possible to quantify risk, mitigate and control risks and individuals who manage and control the asset and risks.

### **How to Identify an IA**

- 1) Does the information have a value to the organisation? i.e.
  - a. How useful is it? Will it cost money to reacquire?
  - b. Would there be legal, reputational or financial repercussions if you couldn't produce it on request?
  - c. Would it have an effect on operational efficiency if you could not access it?
  - d. Would there be consequences for not having it?
- 2) Is there a risk associated with the information? i.e.
  - a. Is there a risk of losing it?
  - b. A risk that it is not accurate?
  - c. A risk that someone may tamper with it?
  - d. A risk arising from inappropriate disclosure?
- 3) Does the class of information have a specific content? i.e.
  - a. Do you understand what it is?
  - b. What it does?
  - c. Does it include the context of the data?
- 4) Does the information have a manageable lifecycle? i.e.
  - a. Are all the components created for a common purpose?
  - b. Have the same retention date
  - c. Be disposed of in the same way and according to the same rules?

### **Privacy Impact Assessments (PIA)**

PIA are a means of assessing risk when processing personal information. They should be conducted at the start of any project collecting personal digital data. There is a statutory need to conduct them where special category data or there is a high risk of data. Further information is included in the PIA template and procedure.

## **Information Security**

Information stored and processed by the council or by third parties working on behalf of the Alun School should be recognised and managed as a valuable asset and subject to the same resource management processes as any other resource. When data is created, stored, transmitted or communicated it must be protected from unauthorised access, use, modification or destruction.

Without adequate levels of protection, confidentiality, integrity and availability of information it is not possible to comply with obligations including legal, statutory and contractual requirements. Personal data should be encrypted or pseudonymised where possible.

All access to, and use of information should follow the information governance principles.

## **Confidentiality**

Appropriate measures must be taken to ensure that information is accessible only to those authorised to have access.

## **Integrity**

The accuracy and completeness of information must be maintained and all changes affecting that information must be authorised, controlled, and validated.

## **Availability**

Information must be available to authorised individuals when required. In the event of a disaster or other events, Alun School information and the systems critical to the success of our organisation must be recoverable in accordance with plans.

## **Authentication**

All persons and systems seeking access to information or to our networked computer resources must first establish their identity to Alun School staff satisfaction.

## **Access Control**

The privilege to view or modify information, computer programs, or the systems on which the information resides, must be restricted to only those whose job functions absolutely require it.

## **Compliance**

User access to information, and activity on the organisations computers, firewalls and networks must be recorded and maintained in compliance with all security, retention, relevant legislation and regulatory requirements.

It is the responsibility of each member of staff to adhere to the School's Security Policies.

## **Information Sharing**

Information sharing is key to the Alun School's goal of delivering better, more efficient services that are coordinated around the needs of the individual. It is essential to enable early intervention and preventative work, for safeguarding and promoting welfare and for wider public protection. Information sharing is a vital element in improving outcomes for all.

## Taking our responsibilities for handling information seriously

At the heart of Information Governance is training. This is so that staff can all understand how managing information affects their working lives and be fully aware of their responsibilities. A key responsibility concerns managing personal protected information. There have been many cases in the public sector of data breaches where staff have lost computers, memory sticks, emailed and faxed personal information to the wrong people. Policies and procedures can be put in place but training helps staff to understand what they are doing and how to implement them.

### Roles

#### Governing Body

The Governing Body is the Data Controller and owns the policy, fulfil a monitoring role, manage complaints and review the policy as appropriate. The Data Protection Officer will provide advice and assistance in these functions.

#### Headteacher (with Data Protection Officer)

Provide an annual update to the Governing Body.

#### Data Protection Officer

To provide an independent overview of compliance issues. Provide advice and assistance when requested and advise and assist on complaints and the operation of the equipment. To monitor the Privacy Impact of the use of CCTV equipment.

#### All staff

Must complete Information Security & Data Protection Training every 12 months to ensure they are compliant in how they use and protect information in their work activities.

School Contact for data protection queries Mrs A. Flint school@alunschool.cymru	Information Commissioner's Office Wycliffe House Water Lane Wilmslow Cheshire SK9 5AF www.ico.gov.uk
Alun School Data Protection Officer:  E2E Education The Annexe, Viscount House River Lane Saltney, Chester CH4 8RH dpo@e2e-education.co.uk 01244 261379	