VENERABLE EDWARD MORGAN CATHOLIC PRIMARY SCHOOL

INFORMATION SECURITY MANAGEMENT POLICY – DATA PROTECTION

This Document is a statement of intent within Venerable Edward Morgan. It was developed through a process of consultation with Key stakeholders and in correspondence with the School's planning and review schedule.

The school aims to safeguard the confidentiality and integrity of its information and to meet it's obligations under the Law. The outcome of the Policy is to protect the School's information from all threats, whether internal or external, deliberate or accidental.

This sets out a framework by which to work.

Approved On:	**25th September 2017**
Next Review:	**September 2018**
Signed:	

"LOVE AND SUPPORT IN ALL WE ARE TAUGHT."
"CARIAD A CHEFNOGAETH YM MHOPETH RHYDAN NI'N DDYSGU."

Introduction

The Data Protection Act 1998 came into force on 1 March 2000, bringing the UK in line with a European Directive on Personal Data (95/46/EC). The Act is there to protect the individual rights and freedoms of individuals, especially their right to privacy with respect to the processing of personal data.

The data Protection Act 1998 requires all organisations, including educational organisations, to hold personal data securely. (See Appendix A)

Terms of the Policy

The School Management Team and Governing Body support the requirements of Information Governance and approve the Information Security Policy.

It is the Policy of the School to ensure that:

a) Confidential and personal information will be protected against unauthorised access
b) Integrity of information will be maintained[1]
c) Regulatory and legislative requirements will be met[2]
d) Information governance maintained and tested
e) Information security education and training will be available to all staff
f) Potential breaches of information security must be reported and investigated

This means for the school that:

- All users of school information systems must be authorised to do so[3]
- Access to systems and data must have appropriate levels of information security
- ***Authorised users will be in possession of a unique user ID and password which must not be shared under any circumstances***
- Business requirements for the availability of information and information systems will be met
- The role and responsibility for managing information security is performed by the Headteacher or designated person who is also responsible for providing advice and guidance on the implementation of this policy
- The Headteacher is directly responsible for implementing the policy within their school and to make all staff aware of their responsibilities under the policy

[1] Safeguarding the accuracy and completeness of information by protecting against unauthorised modification
[2] This includes but is not limited to acting in accordance with the Data Protection Act 1998, Human Rights Act 1998, and Copyright, Designs and Patents Act 1988 and the recommendations of the Caldicott Committee
[3] Ensuring that access to information and information systems is only granted to those who require it to perform their duties – see Appendix E

- It is the responsibility of each employee to adhere to this policy – and all relevant supporting guidelines as applicable[4]
- Access / requests by 3rd parties must be carefully considered before allowing access to data[5]
- All breaches of this policy must be reported immediately to the Lifelong Learning Data Protection Officer or the Principal Learning Officer for ICT
- All serious breaches will be reported to the Information Commissioner's Office (ICO) with the assistance of the LLD Data Protection Officer

Version 1.0

[4] Individuals in breach of this policy and supporting guidelines may be subject to disciplinary procedures
[5] See further guidance: Access to personal information by 3rd parties – Appendix B

Portable Media Policy

Objective: To achieve and maintain appropriate protection of school data

Scope
This Policy applies to all portable devices. It applies to all staff users of the school's ICT systems

Examples include (but not limited to):-
1. Laptops/Notebooks
2. Tablet Devices/iPods/iPads
3. Floppy disks
4. CD ROMs
5. DVDs
6. Memory Sticks
7. External Hard Drives
8. Memory Cards that are present in devices such as mobile phones, digital cameras, PDAs etc
9. Other devices that have the capacity to hold electronic information e.g. MP3 Players, Satellite Navigation Systems etc

Responsibilities
Headteachers are responsible for reporting all lost or stolen portable devices or storage media to appropriate LLD officers in compliance with the ***Reporting Information Security Events*** policy.

Acceptable Use
Personal, confidential or school data must only be stored on encrypted devices (Laptops/Notebooks/USB Memory Sticks) or on the secure network.

Under no circumstances should personal data (as defined by the Data Protection Act) or confidential data be stored on an unencrypted portable device or storage media.

Good practice:
1. Only copy data that you actually need i.e. copy individual files not complete folders; unnecessary rows/columns in spreadsheets must be removed; where possible anonymise data.
2. Ensure that your laptop or memory stick etc. is encrypted.
3. Security is your responsibility at all times. The device must not be left unattended at any time (e.g. in a coat pocket on a hook, in a car, plugged into a PC which is not attended by you, visible on a table or desk). You must endeavour to keep the device securely on your person (use a lanyard). If this is not possible then the device must be locked away securely when unattended.

4. Only transport what is necessary, even information you may not consider to be confidential can be dangerous in the wrong hands.
5. Report any lost or stolen devices to the Headteacher immediately.
6. Only store data for as long as necessary and delete from the device as soon as possible.

Further Advice & Support

Information Governance – Advice and guidance on Information Governance issues can be obtained from the LLD Data Protection Officer.

Breaches of this Policy may result in disciplinary proceedings being brought.

Do's and Don'ts

	Done?
• Do register as Data Controller & register all systems holding personal data with ICO	
• Do read the Information Management Policy, sign up to it and then implement and monitor it	
• Do assign authorised users a unique user ID and password – which then must not be shared under any circumstances	
• Do identify a named individual for managing information security (usually performed by the Headteacher or designated SLT member) who is also responsible for providing advice and guidance on the implementation of this policy	
• Do make all staff aware of their responsibilities under the policy	
• Do advise that it is a responsibility of each employee to adhere to this Information Security Policy and all relevant supporting guidelines	
• Do carefully consider access requests by 3rd parties before allowing access to data	
• Do consider what method you use to deliver personal data – e.g. only use fax as a last resort and use in accordance with guidance	
• Do report all breaches of this Policy immediately to the Lifelong Learning Data Protection Officer or the Principle Learning Officer for ICT	
• Do sign up to the agreement allowing 3rd party access by support staff at the Education ICT Unit to Schools Data	
• Do encrypt all staff memory sticks and non curriculum laptops and record that you have done so	
• Do dispose of redundant ICT equipment according to the guidelines offered i.e. Use the ICT Unit	
• Don't ever store personal sensitive data on an unencrypted mobile device	
• Don't transport data unnecessarily using mobile devices	
• Don't leave confidential material out for others to view whether written, faxed or screen based	
• Don't offer to share data on a pupil to a police officer unless they have submitted an S29 Form signed by a Senior Officer of Rank, Inspector or above	
• Don't e-mail yourself personal sensitive data from your school e-mail account to another personal account	