Information Security Policy 2016-17

As a school we store and handle a significant amount of information on individuals. This information is stored in both paper and electronic forms.

We are committed to ensuring that this information is kept secure and that it is processed correctly and only by the associated personnel with the rights to view that data.

Staff are recommended to refer to national policies for safeguarding individuals' information in paper and electronic formats and the school supports this guidance.

At Ysgol Gyfun Rhydywaun, staff are expected to follow the below guidelines.

Handling Information on Paper

All staff and pupil personal information[1] should be kept in a safe place and individuals must not be able to view this information without authorisation.

Such information should be carried securely if it leaves the school site. Any personal or confidential information should not be left on a desk where others are able to view it.

Teachers have the right to view assessments or any academic information on pupils in the school. They also have the right to view any pastoral information which is deemed to be relevant for them to know in order to effectively teach the pupil, e.g. if there is a medical condition, discipline record etc.

Sometimes, certain pieces of information, e.g. information relating to family background or instances of mistreatment etc will remain confidential. The responsibility of the Head of Progress and Guidance, in co-operation with the Senior Leadership Team, is to determine which information should be revealed and its use should be for educational purposes only.

Electronic Information

Information that is stored on or by pupils and staff should be also be kept confidential.

Staff and pupil personal data is kept on the administration network. Pupils do not have access to this network. Only certain sections of this information is available to staff through the SIMS system. Access to this information is related to the responsibilities held by the member of staff.

Other information is held on the school's curriculum network. There is no access to this network from outside school by pupils or staff other than members of SLT.

[1] See Appendix 1 for definitions of personal information for staff and pupils.

Access to the network is protected by password. Strong passwords (i.e. using punctuation, capitals & numbers) are required for all staff and pupils. Also, pupils are not allowed to use PCs without the permission or supervision of a member of staff.

Guidelines for safeguarding information

Below is a summary of the rules and guidelines:

- You must ensure that it is not possible for others to know individuals' passwords.
- Passwords should be changed regularly.
- Keep any computer equipment safe; ensure that doors to rooms are locked, any portable equipment is in a room or storeroom which is locked. Staff are expected to follow the same rules for equipment which is moved around the school site, e.g. cameras or laptops.
- Pupils and persons who are not members of staff are not allowed to use equipment upon which is stored personal information unless they are under supervision.
- Any data which is stored on portable equipment must be encrypted and secured with a password or other method of securing the data, e.g. biometric means.

Staff are not allowed to transport personal information on pupils or staff on computer equipment which is not protected. If a member of staff needs to transport personal data, e.g. pupil assessments, home, they must store this either on an encrypted laptop or on a flash drive which has been supplied by the school.

Staff must also ensure that safeguarding procedures are in place for information stored on paper, e.g. markbooks etc.

Using the Network, Systems and Equipment at School

School equipment should be used for school activities. However, it is recognised that there are instances when equipment will be used for personal purposes., e.g. to write a personal letter, searching a website to obtain information, searching a website to read personal e-mails.

Staff are allowed to use the school's network, systems and equipment[2] for personal purposes under the following conditions only:

- The use of the equipment does not degrade the equipment.
- The use does not infringe upon learning and teaching.
- The use is during free time.
- The use is appropriate and legal.
- The use is within the expectations of the professional and moral conduct of a member of staff working in a school.
- That the use of consumables does not incur a significant cost to the school. For example, printing of some pages from a website for booking a holiday is allowed, but printing or photocopying tens or hundreds of pages for personal use is not

[2] This applies to use of the Internet, printers, photocopiers etc

allowed. Use of the school's digital cameras are allowed under the above conditions but again the member of staff should purchase new consumable items such as batteries etc.

Use of computer flash and disk drives
Staff are not allowed to transport personal information in an electronic form to or from school unless the data is encrypted or it is possible to ensure the same level of security of that information as if it were stored in paper format.

The school allows the use of flash or disk drives that are not encrypted provided they are used to store non-personal data, e.g. worksheets, policies etc.

The same procedures apply to information stored in the cloud or on personal devices, be they portable or desktop at home.

Monitoring the use of computer systems
The Network Manager regularly monitors what is stored on the school network. This ensures that there are no illegal files e.g. MP3 etc stored on the school network.

Access to staff and pupil workspaces
Teachers have the right to view pupils' workspaces. This is essential and the same as the right a teacher has to view pupils' schoolbooks.

In any institution there has to be at least one individual with access to the whole system. This right is implemented only with the permission of the member of staff or via informing staff, e.g. that a file has been copied to a member of staff's workspace etc.

The persons with access to the whole system for 2011-12 are listed below:

Mark Jones (Headteacher)
Ian Dennett (Network Manager)

Viruses, Adware and Spam
The school has antivirus software on every server and Windows PC. It is a duty of all users of the school systems to reduce the chance of corrupting the school systems with viruses.

Website access is filtered via the Council's web filtering system.

If a member of staff receives a spam e-mail, it should be deleted. If a number of inappropriate e-mails are received, either the Headteacher or the Network Manager should be informed.

Formulated: September 2016,

Personal Information Protection Agreement

I understand the content of this policy and I agree to follow the guidelines indicated in the Information Security Policy.

I also agree to use the school's computer equipment according to the guidelines noted in this policy.

Signed: _____ Date: _____

Appendix 1: Personal Information

The below list is not exhaustive but serves to note examples of the information which is classed as personal or confidential.

Personal data

- Contact details: address, telephone number etc.
- Dates of birth
- Assessments in subjects
- Pictures, videos or sound recordings of staff or pupils.
- Pastoral information

Sensitive personal data

- Medical information
- Personal information such as FSM eligibility, ALN data etc
- Other pastoral information, e.g. behaviour etc
- Information on ethnicity, religious beliefs etc.