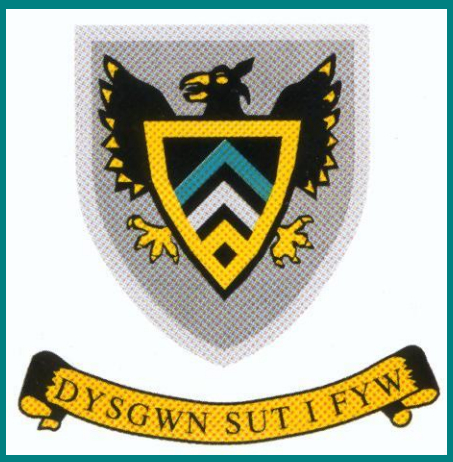
YSGOL GYFUN BRYNTIRION COMPREHENSIVE SCHOOL

INFORMATIION SECURITY POLICY



Information Security Policy

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

At Bryntirion Comprehensive School, staff and governors are expected to follow the guidelines below.

Handling Information on Paper

All staff, governor 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 and governors have the right to view assessments or any academic information on pupils in the school. Teachers 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 Headteacher, 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 pupils and staff should 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 are 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, for example, information relating to assessment data.

Access to the network is protected by password. Pupils are not allowed to use PCs without the permission or supervision of a member of staff.

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

Guidelines for safeguarding information
Please refer to the "Six Simple Rules" document published by BCBC which outlines the good practice in terms of protecting data.

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.
- Staff must not 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 on an encrypted laptop or on an encrypted flash drive which has been supplied by the school. These drives use password based hardware encryption to protect the data.

Staff should ensure that any personal information stored at home has been protected in an adequate manner and it is not possible for other users to view this data.

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

[2] This includes the use of the internet, printers, photocopiers 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.

Members of staff are provided with encrypted flash drives and encryption software can be installed on any laptop by contacting the IT Technician.

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.

The persons with access to the whole system are listed below:

Mr Brain (Headteacher)

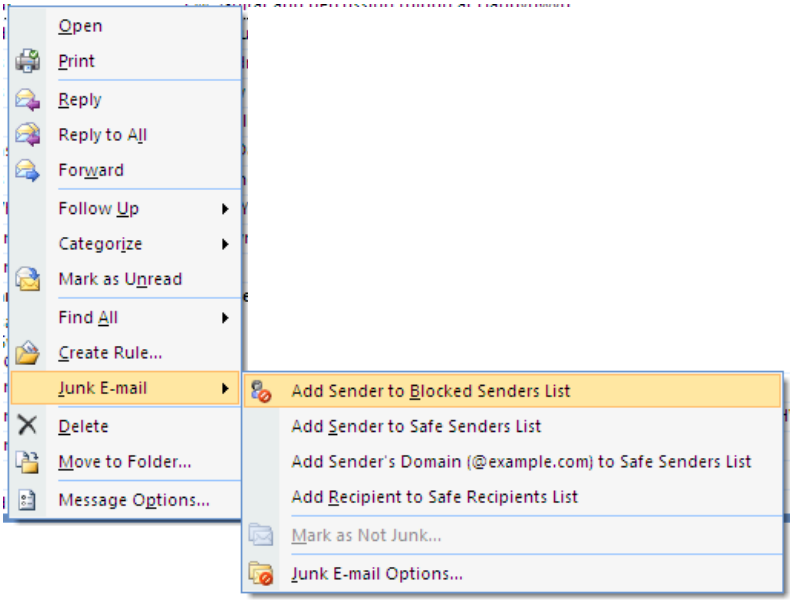
Mr O Jones (Network Manager)

Viruses, Adware and Spam
The school uses either Symantec of McAfee antivirus packages on every PC and laptop. It is a duty of all users of the school systems to reduce the chance of corrupting the school systems with viruses. Personal laptops will only be allowed access to the school network if up-to-date antivirus software is installed.

Website access is filtered via a combination of the Council's web filtering system and our own Bloxx system. These systems monitor and record all website access by pupils and staff.

If a member of staff receives a spam e-mail, it must be deleted and the nature of the e-mail reported to the Network Manager.

It is possible to delete e-mails and prevent the same sender from sending more e-mails via the following method (Microsoft Outlook):


Open
Print
Reply
Reply to All
Forward
Follow Up
Categorize
Mark as Unread
Find All
Create Rule...
Junk E-mail
Delete
Move to Folder...
Message Options...
Add Sender to Blocked Senders List
Add Sender to Safe Senders List
Add Sender's Domain (@example.com) to Safe Senders List
Add Recipient to Safe Recipients List
Mark as Not Junk...
Junk E-mail Options...

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.

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

YSGOL GYFUN
BRYNTIRION
COMPREHENSIVE SCHOOL

Personal Information Protection Agreement

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

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

- I acknowledge receipt of an encrypted flash drive.

Signed: _____ Date: _____