# School Badge.jpg

# Managing eSafety

## Authorising Internet access

All parents must read the school’s ‘Managing eSafety’ document and complete the consent slip before pupils are allowed to use the Internet.

In both Foundation Phase and Key Stage 2, access to the Internet will be by directly supervised access to specific, approved on-line materials.

The school will maintain a current record of all staff and pupils who are forbidden access to the Internet.

## Information system security

* School ICT systems capacity and security are reviewed regularly.
* Virus protection is scheduled to be updated daily.
* Security strategies will be discussed with the school’s ICT support service and the LA Advisory Team.
* Information systems are maintained in line with GDPR. (This policy should be read in conjunction with the ‘School Privacy Notice’)

## E-mail

* Pupils may only use their approved Hwb email addresses.
* Pupils must immediately tell a member of staff if they receive offensive e-mail.
* Pupils must not reveal their personal details or those of others in e-mail communication, or arrange to meet anyone without specific permission.
* E-mail sent to an external organisation should be written carefully and authorized before sending, in the same way as a letter written on school headed paper.

## Published content and the school website

* Pupils personal contact information will not be published.
* The Head teacher will take overall editorial responsibility and ensure that content is accurate and appropriate.

## Publishing pupil’s images and work

* Parental consent will be obtained for the use of photographs on the school website and on the school’s Twitter account.
* Pupils’ full names will not be used on the school website and no names will be associated with images used.
* The school will fully respect the wishes of parents who request that no images of their children are published on the website or on Twitter.

## Social networking and personal publishing

* The school blocks/filters access to social networking sites.
* Newsgroups are blocked unless a specific use is approved.
* Pupils are advised never to give out personal details of any kind which may identify them or their location.
* Pupils and parents are advised that the use of social network spaces outside school is inappropriate for primary aged pupils. This is reinforced through the use of educational materials.

## Managing filtering

The school will work with Conwy County Borough Council to ensure systems to protect pupils are subject to regular checks to ensure that filtering methods are appropriate, effective and reasonable.

If staff or pupils discover an unsuitable site, it must be reported to the e-Safety Co-ordinator who will ensure it is blocked.

## Managing emerging technologies

Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.

Mobile phones are not to be used in school by pupils.

## Assessing risks

The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither the school nor CCBC can accept liability for the material accessed, or any consequences of Internet access. Methods to identify, assess and minimize risks will be reviewed regularly.

The school will audit ICT provision to establish if the e-Safety policy is adequate and that its implementation is appropriate and effective.

## Handling e-Safety complaints

Complaints of Internet misuse will be dealt with by the Headteacher

Responses to Internet misuse may include

* Informing parents/carers
* Removal of Internet/computer access for a set period

Complaints of a child protection nature will be dealt with in accordance with school child protection procedures.