



E-Safety Policy

Contents

Section		Page
1.	Writing and reviewing the e-safety policy	3
2.	Teaching and learning	3
3.	Managing Internet Access	3
4.	Policy Decisions	4
5.	Communications Policy	5

This policy has been written by the school in line with the Vale of Glamorgan Schools Internet Social Networking Policy and Guidance

1. Writing and reviewing the e-safety policy

Our E-Safety Policy has been written by the school, following government guidance. It has been agreed by senior management and approved by governors.

- The e-Safety Policy and its implementation will be reviewed annually.

2. Teaching and learning

Why Internet use is important

- The Internet is an essential element in 21st century life for education, business and social interaction.
- The school has a duty to provide students with quality Internet access as part of their learning experience.
- Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils.

Using the Internet safely to enhance learning

- The school Internet access is filtered at source by the provider.
- Activities that involve the use of the Internet will be age appropriate.
- Pupils using the Internet to search for information will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.
- Pupils will use digital technology safely by agreeing to the [Acceptable Use Agreement](#)
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation
- The school will ensure that the use of Internet derived materials by staff and pupils complies with copyright law.
- Pupils will be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

3. Managing Internet Access

Information system security

- School ICT systems capacity and security will be reviewed regularly in consultation with the school's technician.
- Virus protection will be updated regularly by the school's technician.
- Security strategies will be discussed with the LEA.

E-mail

- Pupils will be taught about e-mail through a virtual learning environment as part of their ICT scheme of work.
- Pupils may only use approved e-mail accounts on the school system.
- Pupils must immediately tell a teacher if they receive an offensive e-mail.
- Pupils must not reveal personal details of themselves or 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 authorised before sending, in the same way as a letter written on school headed paper.
 - Access to external personal e-mail accounts is not permitted.
 - The forwarding of chain letters is not permitted.

Social networking and personal publishing

- The school will not allow access to social networking sites.
- Newsgroups will be blocked unless a specific use is approved.
- Pupils will be advised never to give out personal details of any kind which may identify them or their location.
- Pupils will be advised of the dangers of the use of social network spaces outside school.

Managing emerging technologies

- Emerging technologies will be examined for educational benefit.
- Pupils are not permitted to bring mobile phones into school without permission from an adult.

Protecting personal data

- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.

4. Policy Decisions

Authorising Internet access

- All staff must read and sign the 'Acceptable ICT Use Agreement' before using any school ICT resource.
- Parents will be asked to sign a consent form granting permission for their child to use the internet.
- The school will keep a record of all staff and pupils who are granted Internet access. The record will be kept up-to-date, for instance a member of staff may leave or a pupil's access be withdrawn.
- At Foundation Phase, access to the Internet will be by adult demonstration with occasional directly supervised access to specific, approved on-line materials.

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 the LEA can accept liability for the material accessed, or any consequences of Internet access.
- The school will audit ICT provision to establish if the e-safety policy is adequate and that its implementation is effective.
-

Handling E-Safety complaints

- Complaints of Internet misuse will be dealt with by a senior member of staff.
- Responses to Internet misuse may include informing parents/carers or removal of Internet/computer access for a set period.
- Any complaint about staff misuse must be referred to the headteacher.
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.

Community use of the Internet

- The school will be sensitive to Internet related issues experienced by pupils outside of school, e.g. social networking sites. Appropriate advice and guidance on safe use will be given to pupils.

5. Communications Policy

Introducing the E-Safety policy to pupils

- E-safety rules will be posted in all KS2 classrooms and discussed with the pupils at the start of each year.
- KS2 pupils will be required to sign a responsible use class 'contract'.
- Pupils will be informed that Internet use will be monitored.
- E-safety will be taught through the citizenship strand of the DCF and/or the RSE curriculum.

Staff and the E-Safety policy

- All staff will be given the School E-Safety Policy and its importance explained.
- Staff should be aware that Internet traffic can be monitored. Discretion and professional conduct is essential.

Enlisting parents' support

- Parents' attention will be drawn to the School E-Safety Policy on the school's website.
- A partnership approach will be encouraged. This could include demonstrations for parents/carers provided by the Community Police and suggestions for safe home Internet use.
- The school will maintain a list of E-Safety resources for parents/carers.

Failure to Comply

- Failure to comply in any way with this policy will be considered a serious risk to health and safety and all incidents of non-compliance will be investigated by a senior member of staff.