



# **The Blyth School**

## **Community College**

### **E - SAFETY POLICY**

<b>School Name: The Blyth School</b>
<b>Date Policy Formally Reviewed/Approved By Governors: May 20<sup>th</sup> 2010</b>
<b>Date Policy Becomes Effective: May 20<sup>th</sup> 2010</b>
<b>Review Date (s): May 2011</b>
<b>Person(s) responsible for Implementation and Monitoring: DM AB</b>
<b>Author: AC</b>
<b>Location of Policy: BK Staff Intranet, School Website</b>
<b>Other relevant policies e.g. Child protection, Behaviour Policy</b>

**We are committed to safeguarding and promoting the welfare of children and young people and expects all staff and volunteers to share this commitment.**

## **Policy statement**

E-Safety encompasses internet technologies and electronic communications such as mobile phones and wireless technology. It highlights the need to educate children and young people about the benefits and risks of using new technology and provides safeguards and awareness for users to enable them to control their online experiences.

The school's e-safety policy will operate in conjunction with other policies including those for Student Behaviour, Anti - Bullying, Curriculum, Responsible Internet Use policy and Data Protection policy.

E-Safety depends on effective practice at a number of levels:

- Responsible ICT use by all staff and students; encouraged by education and made explicit through published policies.
- Sound implementation of e-safety policy in both administration and curriculum, including secure school network design and use.
- Safe and secure broadband from Northumberland County Council including the effective management of Forensic software.

### **Writing and reviewing the e-safety policy**

- TBSCC has an e-Safety coordinator.
- The e-Safety Policy and its implementation will be reviewed annually.
- The e-Safety Policy was revised by the Senior Leadership Team on 13<sup>th</sup> May 2010
- It was approved by the Governors on

## **Teaching and learning**

### **Why Internet use is important**

- The Internet is an essential element in 21st century life for education, business and social interaction. TBSCC 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 students.

### **Internet use will enhance learning**

- The school Internet access will be designed expressly for student use and will include filtering appropriate to the age of students.

- Students will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.
- Students will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.

### **Students will be taught how to evaluate Internet content**

- Schools should ensure that the use of Internet derived materials by staff and by pupils complies with copyright law.
- Students should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy

## **Managing Internet Access**

### **Information system security**

- School ICT systems capacity and security will be reviewed regularly.
- Virus protection will be installed and updated regularly.
- Security strategies will be discussed with the Local Authority.

### **E-mail**

- Students may only use approved e-mail accounts on the school system.
- Students must immediately tell a teacher if they receive offensive e-mail.
- Students 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.
- The forwarding of chain letters is not permitted.
- E-mail accounts should not be open on a projected screen at any time.

### **Published content and the school web site**

- The contact details on the Web site will be the school address, e-mail and telephone number. Staff or students personal information will not be published.
- The head teacher or nominee will take overall editorial responsibility and ensure that content is accurate and appropriate.

### **Publishing student images and work**

- Photographs that include students will be selected carefully. No photographs of students whose identity should be kept discrete will be placed on the web – site.
- Students' full names will not be used anywhere on the Web site particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school Web site.
- Work can only be published with the permission of the student and parents.

## **Social networking and personal publishing**

- School will take every available precaution to block/filter access to social networking sites.
- Newsgroups will be blocked unless a specific use is approved.
- Students will be advised never to give out personal details of any kind which may identify them or their location.
- Students must not place personal photos on any social network space.
- Students should be advised on security and encouraged to set passwords, deny access to unknown individuals and how to block unwanted communications. Students should be encouraged to invite known friends only and deny access to others. Details of how to do this are displayed on the school web-site.

## **Managing filtering**

- The school will work in partnership with the LA, DfCS and the Internet Service Provider to ensure systems to protect students are reviewed and improved.
- If staff or pupils discover an unsuitable site, it must be reported to the e-Safety Coordinator or the Network Manager.
- Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

## **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 will not be used during school time. The sending of abusive or inappropriate text messages is forbidden.

## **Protecting personal data**

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

# **Policy Decisions**

## **Authorising Internet access**

- All staff must read and sign the 'Appropriate use policy' before using any school ICT resource.
- The school will maintain a current record of all staff and pupils who are granted access to school ICT systems.
- Secondary students must apply for Internet access individually by agreeing to comply with the Responsible Internet Use statement.
- Parents will be asked to sign and return a consent form.

### **Assessing risks**

- TBSCC will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither the school nor NCC can accept liability for the material accessed, or any consequences of Internet access.
- The school will audit ICT use to establish if the e-safety policy is adequate and that the implementation of the e-safety policy is appropriate.

### **Handling e-safety complaints**

- Complaints of Internet misuse will be dealt with by a senior member of staff.
- Any complaint about staff misuse must be referred to the head teacher.
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.
- Students and parents will be informed of the complaints procedure.
- The handling of potentially illegal issues will be handled in conjunction with Police.

## **Communications Policy**

### **Introducing the e-safety policy to pupils**

- E-safety rules will be posted in all networked rooms.
- Students will be informed that network and Internet use will be monitored.

### **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 and traced to the individual user. Discretion and professional conduct is essential.
- Staff that manage filtering systems or monitor ICT use will be supervised by senior management and have clear procedures for reporting issues.

### **Enlisting parents' support**

- Parents' attention will be drawn to the School e-Safety Policy in correspondence and on the school Web site.