TASKER MILWARD VC SCHOOL

E SAFETY POLICY

Issue No	Author/Owner	Date Written/Reviewed	Approved by Governors on	Comments
Issue 1	HT/SLT	March 2011	10.05.11	
Reviewed	MT-J	Oct 2012		

TASKER MILWARD POLICY FOR E SAFETY

E-Safety Policy

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.

Tasker Milward's e-Safety Policy reflects the need to raise awareness of the safety issues associated with electronic communications as a whole.

The school's e-safety policy will operate in conjunction with other policies including those for BfL, Anti-Bullying, Teaching and Learning, Data Protection and Security.

The Core e-Safety Policy

This core e-safety policy provides the essential basic coverage to protect staff, pupils, the school and PCC.

End to End e-Safety

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, secure and appropriate internet access, including the effective implementation and management of Web filtering.

School e-safety policy

Policy must be translated into practice to protect pupils and educate them in responsible ICT use.

1.1 Writing and reviewing the e-safety policy

The e-Safety Policy is part of the School Improvement Plan and relates to other policies including those for ICT, Anti-Bullying and for Child Protection.

- The HoY will act as e-safety coordinators for their year group (ie concerns re inappropriate content or contact will initially be passed to them) with referral to the designated teacher for Child Protection as appropriate. The responsibility for monitoring the results from 'Securus' rests with the network team.
- Our e-Safety Policy has been written by the school, building on PCC advice and WAG guidance. It has been agreed by senior management and approved by governors.
- The e-Safety Policy and its implementation will be reviewed annually.

1.2 Teaching and learning

1.2.1 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.

1.2.2 Internet use will enhance learning

- The school Internet access will be designed expressly for pupil use and will include filtering appropriate to the pupils.
- Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation

1.2.3 Pupils will be taught how to evaluate Internet content

- The school will ensure that the use of Internet derived materials by staff and by 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.

2.2 Managing Internet Access

2.2.1 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.

2.2.2 E-mail

- Pupils may only use approved e-mail accounts on the school system.
- Pupils must immediately tell a teacher if they receive 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.
- Staff will be provided with an email account for use with pupils and other stakeholders
- Official E-mail to an external organisation sent on behalf of the school as an entity should be written carefully and authorised before sending, in the same way as a letter written on school headed paper. This does not apply to professional e-mail correspondence with colleagues by an individual member of staff.
- The forwarding of chain letters is not permitted.
- Use of email is regulated by the ICT acceptable use policy

2.2.3 Published content and the school web site

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

2.2.4 Publishing pupils' images and work

- Photographs that include pupils will be selected carefully and will not enable individual pupils to be clearly identified.
- Pupils' full names will not be used anywhere on the Web site 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 will only be published with the permission of the pupil and parents.
- Staff should not store images of pupils on personal digital equipment.

2.2.5 Social networking and personal publishing

- School will restrict access to social networking sites.
- 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 potential risks in placing personal photos on any social network space.
- Pupils will be advised on security and encouraged to set passwords, deny access to unknown individuals and how to block unwanted communications. Students will be encouraged to invite known friends only and deny access to others.
- Staff should not accept pupils as friends on social networking sites.

2.2.6 Managing filtering

- The school will work in partnership with the LEA, WAG and the Internet Service Provider and other appropriate agencies to ensure systems to protect pupils are reviewed and improved.
- If staff or pupils discover an unsuitable site, it must be reported to the Network Manager.
- Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.
- Internet filtering capability and relevance will be regularly reviewed by the Network Manager
- Downloads from the Internet will be restricted, authorised downloads will be checked for viruses and malware in line with the ICT system security policy

2.2.7 Managing videoconferencing

- IP videoconferencing should use the educational broadband network to ensure quality of service and security rather than the Internet.
- Pupils should ask permission from the supervising teacher before making or answering a videoconference call.
- Videoconferencing will be appropriately supervised for the pupils' age.

2.2.8 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 lessons or formal school time. The sending of abusive or inappropriate text messages is forbidden, as is the videoing and uploading of inappropriate material.
- Staff will be issued with a school phone where contact with pupils is required. Any necessary contact made by staff should use the school phone and text systems or go through a senior member of staff.

2.2.9 Protecting personal data

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

2.3 Policy Decisions

2.3.1 Authorising Internet access

- All staff must read and sign the 'ICT acceptable use policy' before using any school ICT resource.
- The school will maintain a current record of all staff and pupils who are not granted access to school ICT systems, by exception.
- Pupils 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.

2.3.2 Assessing risks

- The school 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 PCC can accept liability for the material accessed, nor any consequences of Internet access.
- The school should audit ICT use to establish if the e-safety policy is adequate and that the implementation of the e-safety policy is appropriate.

2.3.3 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 headteacher.
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.
- Pupils and parents will be informed of the complaints procedure.
- Discussions will be held with the Police Youth Crime Reduction Officer to establish procedures for handling potentially illegal issues.

2.3.4 Community use of the Internet

- The school will liaise with local organisations to establish a common approach to e-safety.

2.4 Communications Policy

2.4.1 Introducing the e-safety policy to pupils

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

2.4.2 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 will immediately report issues to their Line Manager following school established procedures .

2.4.3 Enlisting parents' support

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