BOURNE COMMUNITY COLLEGE

e-SAFETY POLICY

September 2014

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.

The college's e-safety policy will operate in conjunction with other policies including those for Student Behaviour, Bullying, Curriculum, Data Protection and Security.

e-Safety 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 college network design and use.
- Safe and secure broadband from Capita including the effective management of Websense filtering.

College e-safety policy

2.1 Writing and reviewing the College e-safety policy

The e-Safety Policy is part of the College Strategic Plan and relates to other policies including those for ICT, bullying and for child protection.

- The college will appoint an e-Safety Co-Ordinator.
- Our e-Safety Policy has been written by the college. It has been agreed by senior management and approved by governors.
- The e-Safety Policy and its implementation will be reviewed annually.
- The e-Safety Policy was revised by: Dene Ellis and Janet Murray Brown in July 2014
- It was approved by the Governors in March 2014

2.2 Teaching and learning

2.2.1 Why Internet use is important

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

2.2.3 Internet use will enhance learning

- The college Internet access will be designed expressly for pupil 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

2.2.4 Students will be taught how to evaluate Internet content

- Colleges should ensure that the use of Internet derived materials by staff and by students 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.

2.3 Managing Internet Access

2.3.1 Information system security

- College 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.

2.3.2 E-mail

- Students may only use approved e-mail accounts on the college system.
- Students must immediately tell a teacher if they receive offensive e-mail or cyber bullying.
- Students must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.
- Staff may communicate with students through the wsgfl email system as long as the content complies with professional practice and is related to school issues.

2.3.3 Published content and the college web site

- The contact details on the Web site should be the college address, e-mail and telephone number. Staff or students personal information will not be published.
- Ranjit Verghese , Deputy Headteacher, will have editorial responsibility and ensure that content is accurate and appropriate.

2.3.4 Publishing pupils' images and work

- Photographs that include students will be selected carefully and will not enable individual students to be clearly identified unless permission from students' parents/carers has been obtained.
- Students' full names will not be used anywhere on the Web site or Blog, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of students are published on the college Web site.
- Work can only be published with the permission of the pupil and parents.

2.3.5 Social networking and personal publishing

- College will block/filter access to social networking sites.
- Students will be advised never to give out personal details of any kind which may identify them or their location.
- 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.
- Staff should not befriend current students through social network web sites. Staff are further advised that they should only engage in social media contact with ex-students after the ex-student is 18 years old. Social media contact with ex-students who are still under 18 years of age may be appropriate if the staff member is known to the family through links external to the school.

2.3.6 Managing filtering

- If staff or students 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.

2.3.7 Managing videoconferencing

- IP videoconferencing will be supervised by staff and with known endpoints.
- Students should ask permission from the supervising teacher before making or answering a videoconference call.

2.3.8 Managing emerging technologies

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in college is allowed.
- Use of Mobile phones in lessons will only be allowed for specific purposes as required by the teacher for example, as a camera.
- The sending of abusive or inappropriate text messages is forbidden.

2.3.9 Protecting personal data

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

2.4 Policy Decisions

2.4.1 Authorising Internet access

- All staff must read and sign the ‘Acceptable use policy’ before using any college ICT resource.
- The college will maintain a current record of all staff and students who are granted access to college ICT systems.
- Students must apply for Internet access individually by agreeing to comply with the Responsible Internet Use statement which must be countersigned by parents.

2.4.2 Assessing risks

- The college 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 college computer. Neither the college nor WSCC can accept liability for the material accessed, or any consequences of Internet access.
- The college should audit ICT use to establish if the e-safety policy is adequate and that the implementation of the e-safety policy is appropriate.

2.4.3 Handling e-safety complaints

- Complaints of Internet misuse will be dealt with by the e-safety co-ordinator in the first instance and referred to LT if of a serious nature.
- Any complaint about staff misuse must be referred to the Headteacher.
- Complaints of a child protection nature must be dealt with in accordance with college child protection procedures.

2.5 Communications Policy

2.5.1 Introducing the e-safety policy to students

- E-safety rules will be posted in all networked rooms.
- Students will be informed that network and Internet use will be monitored.
- E- safety will be delivered through the scheme of work for ICT.

2.5.2 Staff and the e-Safety policy

- All staff will be given the College 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.

2.5.3 Enlisting parents' support

- Parents' attention will be drawn to the College e-Safety Policy in newsletters, the college prospectus and on the college Web site.

APPENDIX A

E-Safety Audit – Secondary

This quick self-audit will help the senior leadership team (SLT) assess whether the e-safety basics are in place.

Has the college an e-Safety Policy that complies with CFE guidance?	
Date of latest update:	
The Policy was agreed by governors on:	
The Policy is available for staff :	
And for parents:	
The Designated Child Protection Coordinator is:	
The e-Safety Coordinator is:	
Has e-safety training been provided for both students and staff?	
Do all staff sign an ICT Code of Conduct on appointment?	
Do parents sign and return an agreement that their child will comply with the College e-Safety Rules?	
Have college e-Safety Rules been set for students?	
Are these Rules displayed in all rooms with computers?	
Internet access is provided by an approved educational Internet service provider and complies with DfES requirements for safe and secure access.	
Has the college filtering policy has been approved by LT?	
Has an ICT security audit been initiated by LT, possibly using external expertise?	
Is personal data collected, stored and used according to the principles of the Data Protection Act?	
Are staff with responsibility for managing filtering, network access and monitoring adequately supervised by a member of LT?	