Tibshelf Community School

Online Safety

(Tibshelf Policy)

Policy Status	Date	CHAIR OF COMMITTEE	Minute No:
Accepted by CC&S	24/09/2014		CCS/14/63
Ratified at Full Governors	12/11/2014		GB/14/53
Reviewed by S&C	07 Oct 2015	Steve Marvin	S+C/15/27
Approved by S+C	9 Nov 2016	Steve Marvin	SC/16/36
Approved by Curriculum	18/10/2017	Justin Hawley	CC/10.17-07
Approved by Curriculum	17/10/2018	Justin Hawley	CC/10.18-07

Review Period: 1 Year

Contents

1.0 Introduction

E-Safety encompasses internet technologies and electronic communications such as mobile phones, tablet devices 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, Safeguarding and Data Protection.

The school will hold an E-Safety week and take part in safer internet day.

The school has updated its website to incorporate the CEOP's report abuse icon which allows students and members of the community to report any e-safety concerns.

2.0 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 and taught lessons covering e-safety.
- Sound implementation of e-safety policy in both administration and curriculum, including secure school network design and use.
- The supply of a safe and secure broadband connection with appropriate filtering and connectivity will be supported by the network manager as part of their role.
- Student activity is monitored and filtered on the internet.
- E-mail filtering will be provided through the school IT management and monitoring systems.

3.0 E-Safety at Tibshelf Community School

- Our E-Safety Policy has been agreed by senior management and approved by governors.
- An e safety team will monitor its implementation and effectiveness. This team will include student e safety ambassadors and staff trained on the CEOP's Champions Course.

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

4.0 Teaching and Learning

All students will complete an e-safety unit of work through PSHE in Years 7, 8 and 9. The Scheme of Work will be regularly updated to reflect the changes in emerging technologies.

E-safety will also be promoted during tutor time by form tutors on a regular basis.

E-safety is taught at KS3 as part of the ICT Curriculum.

4.1 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 students.

4.2 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.

4.3 Students will be taught how to evaluate Internet content

- School 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.

5.0 Managing Internet Access

5.1 Information system security

- School ICT systems capacity and security will be reviewed regularly.
- Virus protection will be installed and updated regularly.

- The results of misuse collected by school monitoring systems will be reviewed and the necessary steps be taken with those breaking rules.

5.2 E-mail

- All Students and Staff have a network account and individual email address.
- Students must immediately tell a teacher if they receive offensive e-mail who will report this to the relevant member of staff.
- Staff must report any incidents of internet abuse to the appropriate member of staff or senior leader.
- 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 in the same way as a letter written on school headed paper.
- The forwarding of chain letters is not permitted.

5.3 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 student's personal information will not be published although pictures of students may be accessible.

- The member of the leadership team with responsibility for ICT will take overall editorial responsibility and ensure that content is accurate and appropriate.

5.4 Publishing Student's images and work

- Photographs that include Students will be selected carefully
- Written notice will be given to all parents on an annual basis with regard to photographs of students being published on the school web site and other school publications.
- Student's work can only be published with the permission of the student and parent.

5.5 Social networking and personal publishing

- 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 must not post any information or images related to staff in school.
- Students 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.
- Students will receive regular updates on concerns and issues in assemblies and form tutor time to reinforce the importance of online safety.

5.6 Managing emerging technologies

- Emerging technologies will be examined for educational benefit and risk assessed before use in the school is allowed.
- Mobile phones will be switched off during lessons or other formal school times unless they are being used appropriately for educational use in lessons.
- The use of mobile technology to send abusive or inappropriate text messages or email is forbidden as is the videoing or photographing of students or staff without permission.

5.7 Protecting personal data

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

6.0 E Safety Ambassadors/Champions

- The school will appoint a team of e-safety ambassadors who are trained to work with staff (CEOP's Champions) and students on e-safety issues
- E-safety ambassadors will pass on concerns to the Deputy Headteacher or ICT and/or the senior designated person any concerns that directly relate to the safety of a student.
- E-safety ambassadors will run a series of drop in sessions and events including assemblies to promote the safe use of online environments.
- The e-safety ambassadors will promote the use of the CEOP's logo on the website as a method of reporting concerns.

- There will be regular assemblies on current issues related to e-safety which will be age appropriate to highlight and raise awareness of risks.

7.0 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.

8.0 Introducing the e-safety policy to Students

- E-safety rules will be available to all students through for tutors.
- Students will be informed that network and Internet use will be monitored.

9.0 Staff and the e-Safety policy

- 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.

10.0 Enlisting Parents' Support

- Parents' attention will be drawn to the school E-Safety Policy in newsletters, and via other appropriate events
- Parents will be able to access the relevant areas of the school website where necessary.
- E-Safety Champions will offer parent events to raise awareness of parents to the risks related to use of the internet.

11.0 Regulations Which Govern The Use of ICT Facilities

Below are details of some of the main Acts of Parliament as at March 2003 which govern the use of ICT facilities.

The Regulation of Investigatory Powers Act 2000

This Act updates the Interception of Communications Act to take account of technological change such as the growth of the Internet.

It establishes a new legal framework to govern the interception of communications. The Act sets the rules regarding activities such as recording, monitoring or diverting communications in the course of their transmission over a public or private telecoms system.

http://www.legislation.hmso.gov.uk/acts/acts2000/20000023.htm

The Computer Misuse Act (1990)

This makes both the unauthorised use of a computer system and the unauthorised modification of computer data a criminal offence. Also unauthorised access to a computer system with intent to commit or facilitate the commission of a serious crime is an offence under this Act.

http://www.legislation.hmso.gov.uk/acts/acts1990/Ukpga_19900018_en_1.htm

The Data Protection Act (1998)
This Act compels Tibshelf Community School to take specific measures to ensure that all personal information held about living (identified or identifiable) individuals is processed according to eight Data Protection Principles.

The Act allows individuals to obtain a copy of their own personal data, the right to have inaccurate personal data corrected or erased and, where appropriate, to seek redress for any damage caused. In addition, the Act obliges Tibshelf School to provide a complete description of all personal data held by Tibshelf School, their uses, purposes, disclosures and sources, to the Office of the Information Commissioner. The Act provides for criminal offences if these obligations are neglected.

http://www.legislation.hmso.gov.uk/acts/acts1998/19980029.htm

The Copyright, Designs and Patents Act (1988) & The Copyright, etc. and Trade Marks (Offences and Enforcement) Act 2002
For copyright purposes, computer programs are defined as 'literary works' and are the subject of the many restrictions designed primarily to control the use of printed work. All computer software, whether covered by a specific licence or not, is copyrighted under this Act.

http://www.legislation.hmso.gov.uk/acts/acts1988/Ukpga_19880048_en_1.htm

The Copyright, etc. and Trade Marks (Offences and Enforcement) Act 2002
http://www.legislation.hmso.gov.uk/acts/acts2002/20020025.htm

This Act compels Tibshelf School to take specific measures to ensure that all personal information held about living (identified or identifiable) individuals is processed according to eight Data Protection Principles.

The Act allows individuals to obtain a copy of their own personal data, the right to have inaccurate personal data corrected or erased and, where appropriate, to seek redress for any damage caused. In addition, the Act obliges Tibshelf School to provide a complete description of all personal data held by Tibshelf School, their uses, purposes, disclosures and sources, to the Office of the Information Commissioner. The Act provides for criminal offences if these obligations are neglected.

http://www.legislation.hmso.gov.uk/acts/acts1998/19980029.htm

The Copyright, Designs and Patents Act (1988) & The Copyright, etc. and Trade Marks (Offences and Enforcement) Act 2002
For copyright purposes, computer programs are defined as 'literary works' and are the subject of the many restrictions designed primarily to control the use of printed work. All computer software, whether covered by a specific licence or not, is copyrighted under this Act.

http://www.legislation.hmso.gov.uk/acts/acts1988/Ukpga_19880048_en_1.htm

The Copyright, etc. and Trade Marks (Offences and Enforcement) Act 2002
http://www.legislation.hmso.gov.uk/acts/acts2002/20020025.htm

http://www.legislation.hmso.gov.uk/acts/acts2000/20000007.htm

The Obscene Publications Act (1959), the Protection of Children Act (1978) and the Criminal Justice Public Order Act (1994)
These Acts protect against pornography and indecent images of children.

http://www.hmso.gov.uk/acts/acts1994/Ukpga_19940033_en_1.htm

Health and Safety at Work Act (1974), including the Control of Substances Hazardous to Health (COSHH) Regulations (1988)
This regulates safety in the workplace and contains a number of clauses pertinent to the IS/IT environment, such as, the Display Screen Equipment Regulations (1992).

Criminal Justice and Police Act (2001)
This provides for combating crime & disorder. It makes provision for the disclosure of information relating to criminal matters and the power of search & seizure. This Act amends The Police and Criminal Evidence Act 1984.

http://www.hmso.gov.uk/acts/acts2001/20010016.pdf

The Defamation Act (1996)
This makes it an offence to cause libel or slander as a result of information stored on the World Wide Web, or transmitted via a telecommunications system such as the Internet

http://www.hmso.gov.uk/acts/acts1996/1996031.htm