Alsager School

An Achieving School - A Caring Community

E-SAFETY POLICY

REVIEW DATE: DECEMBER 2017

Prepared by Ellen Walton

December 2016

PRESENTED TO THE PUPIL PROGRESS COMMITTEE ON FEBRUARY 15TH 2017 AND SUBSEQUENLTY APPROVED AND ADOPTED ON THE SAME DATE

Chair of Pupil Progress Committee: Shirley Jones

Signature: S. Shirley Jones

Date: 15/2/17

E-SAFETY POLICY REVIEW DATE: DECEMBER 2017

Rationale

E-Safety encompasses Internet and related electronic communications such as mobile phones and wireless technology. It highlights the need to educate our students 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 breadth of issues classified within online safety is considerable, but can be categorised into three areas of risk:

- content: being exposed to illegal, inappropriate or harmful material;
- contact: being subjected to harmful online interaction with other users; and
- conduct: personal online behaviour that increases the likelihood of, or causes, harm

Page 62 Keeping Children Safe in Education

Purpose

The purpose of Internet use at Alsager School and Sixth Form College is to raise educational standards, to promote student achievement, to support the professional work of staff and to enhance the school's management information and administration systems. Internet use is part of the statutory curriculum and a necessary tool for learning. It is an essential element in 21st century life for education, business and social interaction. Access to the Internet is therefore an entitlement for students who show a responsible and mature approach to its use. The Governors and Headteacher at Alsager School takes seriously the responsibility to provide our students with high quality Internet access. The students will use the Internet outside school and, together with their parents, will need to learn how to evaluate Internet information safety and to take care of their own safety and security when on line.

E-Safety Policy

An effective e-Safety policy is required to ensure that staff, students and Governors at Alsager School are able to use the internet and related communications technologies appropriately and safely.

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 and secure broadband from Exa Network in addition to an effective web filtering system called Iboss.
- These processes are shared annually via the e-safety champions' action plan, e-safety lessons in Co-operative Learning lessons and competitions, e-safety assemblies, IT lessons, staff training and via the Acceptable Use signed by all IT users within school.

Contributors

Alsager School's e-Safety Policy has been compiled by Ellen Walton (Designated Safeguarding Lead), Lee Martin (IT systems Manager), Neil Williams (Assistant Headteacher i/c IT systems) and the E-safety Champions who lead their peers on e-safety.

This policy is based on the updated Keeping Children Safe in Education 2016 and is to be read in conjunction with the school's Safeguarding and Child Protection Policy, Anti-Bullying Policy and the School's Acceptable Use policy and the Staff Social Networking Guidelines.

1. Teaching and Learning

1.1 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.

1.2 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 the 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 safe and effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.

1.3 Students will be taught how to evaluate Internet content

- As a school we will ensure that the use of Internet derived materials by staff and students complies with copyright law.
- Students will be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

2. Managing Internet Access

2.1 Information System Security

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

2.2 E-mail

- 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.
- School e-mail should not be used for personal purposes.
- Students in Years 7-11 cannot receive or send e-mails from external providers due to the secure security settings established by the school. However, Sixth form students need this provision for the UCAS and employment process. Students are made aware of this via the processes as outlined in the 'End to End' safety section.

2.3 Published content and the school website

- The contact details on the Web site are the school address, e-mail and telephone number. Staff or students personal information will not be published.
- Editors of the website will take responsibility for the accuracy and appropriateness of published information.

2.4 Publishing Student Images and work

- Students work will form a crucial part of Sharepoint.
- Student images will only be used if the school has the permission of the student and his/her parent.

2.5 Social Networking and Personal Publishing

- School currently block/filter access to social networking sites from within the school system.
- Students will be advised via the school's e-safety work within the curriculum never to give out personal details of any kind which may identify them or their location.
- Students will also 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.
- Students do not have any access to Social Networking within school but as a school we do educate the students on how to stay safe online, to maintain security settings and to ensure that they do not share personal information online. All of these are addressed via the channels identified in 'End to End e-safety'.
- Staff should not accept as a "friend" on a social networking site any student currently in the school. The only exception being if they know the student through another context. For example: if they are related. All staff are subject to and sign Alsager school's 'Social Networking Guidelines'.

2.6 Managing filtering

- The school works in partnership with IBOSS and Exa to ensure systems to protect students are reviewed and improved.
- If staff or students discover an unsuitable site, it must be reported to a member of staff who will inform the IT Systems Manager.
- Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

2.7 Managing Video Conferencing

- Staff have access to this facility but this is clearly monitored by the IT Systems Manager.

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 on site during the school day as per our Uniform and Mobile Phone policy. Should mobile phones be used they are confiscated. The sending of abusive or inappropriate text messages is forbidden and students are educated on the risks of sexting through Co-operative Learning, assemblies and the Pastoral System. Staff are well aware that it could be used as a tool for 'peer on peer' abuse.
- Staff will be issued with a school phone when communication is required eg school trips.
- Students should use school cloud spaces for work that needs to be accessed within school. Teacher are advising students to do this.

2.9 Protecting Personal Data

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

3. Policy Decisions

3.1 Authorising Internet access

- The school system will ensure that annually all staff and students must read and digitally sign the "Acceptable Use Policy" before using any school ICT resource.
- The school will maintain a current record of all staff and students who are not allowed access to school ICT systems.
- It is at the schools discretion if a student's email and internet access is withdrawn.

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. The school cannot 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.

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 will be referred to the headteacher.
- Complaints of a Child Protection or Safeguarding nature will be dealt with in accordance with school's Child protection and Safeguarding Policy.

Safeguarding procedures.

- Students and parents will be informed of the complaints procedure.
- Discussions will be held with the Police to establish procedures for handling potentially illegal issues.

3.4 Guest use of the Internet

- This is restricted to internet access only. They are subject to the same school wide filtering. Guest access has short term password access.
- Guests are also asked to sign our 'Acceptable Use Policy' before they access IT within school.

Communications Policy

3.5 Introducing the e-safety policy to students

- This e-safety policy was produced in collaboration with the e-safety champions and was discussed with all Student Councils
- E-safety guidance is displayed on our e-safety board and within IT classrooms.
- Students will be informed that network and Internet use will be monitored.
- Our E-safety champions are CEOP trained and lead their peers on e-safety through workshops and helping to deliver staff training.

3.6 Staff and the e-Safety policy

- All staff will be given access to 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 the Senior Leadership Team and have clear procedures for reporting issues.

3.7 Enlisting parents' support

- Parents' attention will be drawn to the School e-Safety Policy in School Matters and through the school Web Site which includes a range of guidance and support materials.
- The school will provide support to parents in how to support their children online through the Digital Parents magazine and e-safety workshops.