St Anne's Academy

E-Safety Policy

Reviewed and approved by	Endorsed by (if appropriate)	Date of next review
Assets Committee 18 Sept 2014	N/A	Autumn Term 2018

E-Safety Policy

Introduction

The mission and philosophy of the Academy is:

- To be an inspirational community for lifelong learning, underpinned by Christian faith, values, principles and ethos
- To be an inclusive centre of learning
- To recognise the unique value and individuality of every person and to provide personalised learning routes, coaching and support for everyone
- To model high expectations
- To assist and support the regeneration and transformation of the local community.

This policy, and its associated procedures and protocols, is based on these key principles.

All references in this document to the Local Authority/School means the Governing Body of St Anne's Academy.

Contents

1 Definition

E-safety encompasses Internet technologies and electronic communications such as mobile phones as well as collaboration tools and personal publishing. It highlights the need to educate students about the benefits and risks of using technology and provides safeguards and awareness for users to enable them to control their online experience. The Academy seeks to enable students to become digital citizens comfortable using a variety of online tools and with the digital skills needed to enhance their employability.

The Academy's e-safety policy will operate in conjunction with other policies including those for Positive Behaviour, Child Protection, Anti-Bullying, Curriculum, Mobile Phone, Data Protection and Security.

2 Effective Practice

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 Academy network design and use.
- Safe and secure broadband including the effective management of filtering.
- National Education Network standards and specifications.
- E-safety is not the responsibility of the ICT teaching staff or the technicians. ICT and the digital world affect every subject and every member of staff. All staff must use every opportunity to reinforce safe "digital" behaviour particularly by modelling good practise.

3 Academy E-Safety Policy

3.1 Writing and reviewing the e-safety policy

- The e-safety Policy relates to the Academy's safeguarding policies and practices as well as to other policies including those for Anti-Bullying, Mobile Phones, Data Protection and Child Protection.
- The Academy will appoint an e-safety Coordinator who is a member of SLT.
- Our e-safety Policy has been written by the Academy, building on government guidance and is reviewed by the Governing Body.

3.2 Teaching and Learning

3.2.1 Why Internet use is important

- The Internet is an essential element in 21st century life for education, business and social interaction. The Academy 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.
- The purpose of Internet use in Academy is to raise educational standards, to promote student achievement, to support the professional work of staff and to enhance the Academy's management functions.

3.2.2 Internet use will enhance learning:

- The Academy's 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 in the classroom.
- Students will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.

3.2.3 Students will be taught how to evaluate Internet content

- The Academy will ensure that the use of Internet derived materials by staff and 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.
- Students use the Internet widely outside Academy and will need to learn how to evaluate Internet information and to take care of their own safety and security.

3.3 Managing Internet Access

3.3.1 Information system security

- Academy ICT systems capacity and security will be reviewed regularly.
- Virus protection will be updated regularly and automatically.
- Security strategies will be regularly updated in discussion with the Managed Service provider.
- Internet access will be planned to enrich and extend learning activities.
- Access levels will be reviewed to reflect the curriculum requirements and age of students.
- Staff should guide students in on-line activities that will support the learning outcomes planned for the students' age and maturity.

3.3.2 E-mail

- Students may only use approved e-mail accounts on the Academy 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 Academy headed paper.
- The forwarding of chain letters is not permitted.

3.3.3 Publishing Students' images and work

- Photographs that include students will be selected carefully and will not enable individual students to be clearly identified.
- Student's work and photographs can only be published with the permission of the student and parents.

3.3.4 Social networking and personal publishing

- The Academy will block/filter access to social networking sites; this filtering will take account of student's age and educational needs.
- 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. Examples would include real name, address, mobile or landline phone numbers, Academy attended, e-mail address, full names of friends, specific interests and clubs etc.

3.3.5 Managing filtering

The Academy will work with the LA, DFS and the Internet Service Provider to ensure systems to protect students are reviewed and improved. If staff or students discover an unsuitable site, it must be reported to the e-safety Coordinator or a member of the Academy Leadership Team. Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

All users must be aware that all usage of Academy ICT equipment is monitored using sophisticated software. Students' usage is monitored by the LICT Mentor, adults' use is monitored by SLT.

3.3.6 Managing emerging technologies

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in Academy is allowed.
- Students are not allowed mobile phones in class, unless handed to staff for safe keeping. (See mobile phone policy for more detail)
- If necessary, staff will be issued with an Academy phone where contact with Students is required.

3.3.7 Protecting personal data

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998. (See Data Protection Policy)

3.4 Policy Decisions

3.4.1 Authorising Internet access
All users must read and sign the 'Acceptable ICT Use Agreement Staff Appendix 1' or 'Acceptable ICT Use Agreement Student Appendix 2' before using any Academy ICT.
The Academy will keep a record of all users and students who are granted Internet access. The record will be kept up-to-date, for instance a member of staff may leave or a student's access be withdrawn. Parents will be asked to sign and return a consent form.

3.4.2 Assessing risks
The Academy will take all reasonable precautions to ensure that users access only appropriate material. Due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a Academy computer. The Academy can not accept liability for the material accessed, or any consequences of Internet access.

3.4.3 Handling e-safety complaints
Complaints of Internet misuse will be dealt with by a member of SLT. Any complaint about staff misuse must be referred to the Principal.

Complaints of a child protection nature must be dealt with in accordance with Academy child protection procedures.

Students and parents will be informed of the complaints procedure. Some exemplar issues and sanctions for both staff and students are contained within Appendix 3.

3.5 Communications Policy

3.5.1 Introducing the e-safety policy to students
E-safety rules will be posted in all class rooms and discussed with the students at the start of each term. Students will be informed that network and Internet use will be monitored.

3.5.2 Staff and the e-safety policy
All staff will be directed to the Academy e-safety Policy and its importance explained. Regular training and updates will be given to staff and students. Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.

It is recommended that all staff read, understand and abide by the guidance from the local authority about the use of social media sites (See Appendix 4) LA Guidelines on Social Networking)

3.5.3 Enlisting parents' support
Parents' attention will be drawn to the Academy e-safety Policy in newsletters and the Academy website.