



# E-SAFETY POLICY

SANDON PRIMARY ACADEMY & LITTLE SANDON

Mrs R Beckett (Principal)

Review date: September 2023

## **Introduction**

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 pupils about the benefits and risks of using technology and provides safeguards and awareness for users to enable them to control their online experience.

The school's e-safety policy will operate in conjunction with other policies including Child Protection and Anti-Bullying.

## **The CFE Core e-Safety Policy**

The Schools e-Safety Policy Guidance and Template available on SCORE E-safety mini-site ([www.sgfl.org.uk/e-safety](http://www.sgfl.org.uk/e-safety)) provides a full discussion of e-safety issues and links to further information.

This mini-site also provides staff, parents, pupils and governors with information and resources relating to current e-safety issues and practice.

## **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 the Stoke-on-Trent Education WAN including the effective management of Websense filtering.
- National Education Network standards and specifications.

## **Further Information**

C&YPs ICT Curriculum Team

e-Safety materials and Curriculum e-safety advice

01782 236271

[www.sgfl.org.uk/e-safety](http://www.sgfl.org.uk/e-safety)

# School e-safety policy

## 2.1 Writing and reviewing the e-safety policy

The e-Safety Policy is part of the Development Plan and relates to other curriculum and academy policies.

- *Our e-Safety Policy has been written by the school, building on the Stoke-on-Trent e-Safety Policy and government guidance. It has been agreed by senior management and approved by governors*
- *Mrs Heavey will act as the school's e-safety Co-ordinator as this role overlaps with that of Safeguarding Lead*
- *The e-Safety Policy and its implementation will be reviewed regularly.*
- *The e-Safety policy was written in January 2015*
- *It was approved by Governors on: 29 January 2015*

## 2.2 Teaching and learning

### **Why are new technologies and Internet use important**

- *The Internet is an essential element in 21st century life for education, business and social interaction. As an academy, we have 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 is a necessary tool for staff and pupils.*

### **Internet use will enhance learning**

- *The academy Internet access will be designed expressly for pupil use and will include filtering appropriate to primary age pupils.*
- *Pupils will be taught what Internet use is acceptable and what is not and will be given clear objectives for Internet use.*
- *Internet access will be planned to enrich and extend learning activities. Access levels will be reviewed regularly to reflect curriculum requirements and the age of pupils.*
- *Staff should guide pupils in on-line activities that will support planned learning outcomes, as appropriate for pupils' age and maturity.*
- *Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation*

### **Pupils will be taught how to evaluate Internet content**

- *The academy will ensure that the copying and subsequent use of Internet derived materials by staff and 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.*

## **Pupils will be taught how to stay e-safe**

- *Curriculum planning will include age-appropriate opportunities to discuss, role play and learn about the benefits and risks offered by new technologies, such as email, mobile phones and social networking sites.*
- *The teaching of e-safety will begin when the children enter the academy. It will develop in each year group to ensure full coverage of the relevant issues. This coverage will be reviewed regularly to take into account the changing experiences and knowledge of our children e.g. the use of mobile phones by younger pupils.*
- *E-safety rules will be established with each class and their teacher at the start of every academic year. These rules will be on display in the classroom for referral to throughout the year.*

## **Managing Internet Access**

### **Information system security**

- *Academy ICT systems capacity and security will be reviewed regularly*
- *Virus protection will be updated regularly on all networked computers*
- *Security strategies will be in line with current LA advice and practice*

### **E-mail**

- *Pupils may only use approved e-mail accounts on the academy 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*

### **Published content and the school web site**

- *The contact details on the Web site should be the academy address, e-mail and telephone number. Staff or pupils' personal information will not be published*
- *E-mail addresses will be published carefully, to avoid spam harvesting*
- *The Principal will take overall editorial responsibility and ensure that content is accurate and appropriate*

## **Publishing pupil's 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 or Blog, particularly in association with photographs.*
- *Written permission from parents or carers will be obtained before photographs of pupils are published on the academy Web site*

## **Social networking and personal publishing**

- *The academy will block access to social networking sites, except those specifically purposed to support educationally approved practice.*
- *Newsgroups will be blocked unless a specific use is approved.*
- *Pupils will be advised never to give out personal details of any kind which may identify them or their location.*
- *Pupils and parents will be advised that the use of social network spaces, outside school-based controlled systems (i.e. SCORE/ Learning Platform) is inappropriate for primary aged pupils, unless strictly supervised.*
- *Staff and pupils are advised not to publish specific and detailed private thoughts on social networking sites*

## **Managing filtering**

- *The academy will work with Stoke-on-Trent City Council, Becta and the WAN Managed Service Provider to ensure systems to protect pupils are reviewed and improved.*
- *If staff or pupils discover an unsuitable site, the URL must be reported to the ICT Co-ordinator and the ICT Technician, who will act as soon as possible to block the site.*
- *Senior staff will ensure that regular checks are made to ensure that our filtering methods are appropriate, effective and reasonable.*

## **Managing videoconferencing**

- *Full IP videoconferencing should use the educational broadband network to ensure quality of service and security rather than the Internet.*
- *External IP addresses will not be made available to other sites.*
- *Videoconferencing contact information will not be put on the school website.*
- *Academy videoconferencing equipment will not be taken off school premises without permission, since its use over a non-educational network (e.g. the internet) cannot be monitored or controlled.*

## **Users**

- *Parental permission must be given before children can participate in a videoconference call*
- *Pupils must ask permission from the supervising teacher before making or answering a videoconference call*
- *Videoconferencing will be appropriately supervised for the pupils' age*

## **Content**

- *The academy will check that other videoconference participants are delivering material that is appropriate for the class*

## **Managing emerging technologies**

- *Emerging technologies will be examined for educational benefit and protocols will be established before use in school is allowed. These protocols will follow guidance given by the LA*
- *Mobile phones will not be used during lessons or formal school time, unless specifically allowed to support learning as identified by the teacher. The sending of abusive or inappropriate text messages is forbidden*
- *Staff will be issued with a school phone where contact with pupils is required*

## **Protecting personal data**

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

## **Policy Decisions**

### **Authorising Internet access**

- *The academy will maintain a record of all staff and pupils who are granted access to the school's electronic communications, which includes internet access. This record will be kept up-to-date, for instance a member of staff may leave or a pupil's access be withdrawn*
- *At Key Stage 1, access to the Internet will be by adult demonstration or by directly supervised access to specific, approved on-line materials*
- *Parents will be asked to sign and return a consent form.*
- *Sanctions for inappropriate use will be drawn up and shared with staff and pupils*

### **Assessing risks**

- *The academy will take all reasonable precautions to ensure that users access only appropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on an academy computer. Neither the academy nor Stoke-on-Trent City Council can accept liability for the material accessed, or any consequences of Internet access*
- *The academy will audit ICT provision to establish if the e-safety policy is adequate and that its implementation is effective*
- *The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990*
- *Methods to identify, assess and minimise risks will be reviewed regularly*

### **Handling e-safety complaints**

- *E-safety complaints/issues must be reported to the supervising teacher immediately.*
- *Complaints of Internet misuse will be dealt with by a senior member of staff.*
- *Any complaint about staff misuse must be referred to the principal.*

- *Complaints of a child protection nature must be dealt with in accordance with child protection procedures.*
- *Pupils and parents will need to work in partnership with staff to resolve issues.*
- *Sanctions will include:*
  - *Interview by a member of the Management Team*
  - *Informing parents/carers*
  - *Removal or restriction of internet or computer access for a specified period of time*

### **Community use of the Internet**

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

### **Cyberbullying – Understanding and addressing the issues**

The age of children making proficient use of communication technologies is ever decreasing. Therefore, the opportunities for pupils to bully or be bullied via technology, such as email, texts or MSN, are becoming more frequent.

- *The academy will monitor regularly the ICT experience of its pupils in order to provide appropriate training and guidance on cyberbullying*
- *Cyberbullying will be addressed in ICT, PSHCE and other relevant lessons*
- *Pupils, parents, staff and governors will be made aware of the consequences of cyberbullying*
- *Parents will be provided with an opportunity to find out more about cyberbullying through meetings and printed guidance*

### **Cyberbullying – How will risks be assessed?**

- *The academy will take all reasonable precautions to ensure against cyberbullying. However, due to the global and connected nature of new technologies, it is impossible to guarantee that inappropriate use via a school computer will never occur. Neither the academy nor Stoke-on-Trent City Council can accept liability for inappropriate use, or any consequences resulting outside of the academy.*
- *The academy will actively engage with pupils in preventing cyberbullying by:*
  - *Understanding and talking with pupils about cyberbullying e.g. inappropriate use of e-mail, text messages etc*
  - *Keeping existing policies and practices up-to-date with new technologies*
  - *Ensuring easy and comfortable procedures for reporting cyberbullying*
  - *Promoting the positive use of technology*
  - *Evaluating the impact of prevention activities*
- *Records of any instances of cyberbullying will be kept, in line with procedures for other types of bullying incidents. These records will be used to monitor the effectiveness of the academy's prevention activities.*

### **How will cyberbullying reports/issues be handled?**

- *Complaints of cyberbullying will be dealt with by a member of the Senior Management Team*
- *Any complaint about staff misuse must be referred to the Principal*
- *Evidence of offending messages, pictures or online conversations will be kept, in order to demonstrate to others what is happening. This evidence can be used by the academy, internet service provider, mobile phone company or the police to investigate the cyberbullying.*
- *Pupils and parents will need to work in partnership with staff to resolve issues.*

*Sanctions will include:*

- *Interview by a member of the Senior Management Team*
- *Informing parents/carers*
- *Removal of internet or computer access for a specified period of time*

## **Communications Policy**

### **Introducing the e-safety policy to pupils**

- *E-safety rules will be posted in all classrooms and discussed with pupils at the start of each year and as the need arises*
- *Pupils will be informed that network and Internet use will be monitored*
- *Instruction in responsible and safe use should precede Internet access*
- *An e-Safety module will be included in the ICT scheme of work covering both academy and home use*

### **Staff and the e-Safety policy**

- *All staff will be given the academy e-Safety Policy and its application and importance explained*
- *All staff will be informed that all computer and Internet use will be monitored. Discretion and professional conduct is essential*
- *Staff training in safe and responsible Internet use and on the academy e-Safety Policy will be provided as required*
- *Staff that manage filtering systems or monitor ICT use will be supervised by senior management and have clear procedures for reporting issues*

### **Enlisting parents' support**

- *Parents' attention will be drawn to the academy e-Safety Policy in newsletters, the school brochure, on the school website and through parents' sessions.*
- *Internet issues will be handled sensitively, and parents will be advised accordingly.*
- *A partnership approach with parents will be encouraged. This may include parent evenings with demonstrations and suggestions for safe home Internet use.*
- *Advice on filtering systems and educational and leisure activities that include responsible use of the Internet will be made available to parents.*



## Appendix 1: Internet use - Possible teaching and learning activities

Activities	Key e-safety issues	Relevant websites
Creating web directories to provide easy access to suitable websites.	<p>Parental consent should be sought.</p> <p>Pupils should be supervised.</p> <p>Pupils should be directed to specific, approved on-line materials.</p>	<p>Web directories e.g.</p> <p>Networked favourites</p> <p>Ikeepbookmarks.com</p> <p>SCORE minisites</p>
Using search engines to access information from a range of websites.	<p>Parental consent should be sought.</p> <p>Pupils should be supervised.</p> <p>Pupils should be taught what internet use is acceptable and what to do if they access material they are uncomfortable with.</p>	<p>Web quests e.g.</p> <ul style="list-style-type: none"> <li>- Ask Jeeves for kids</li> <li>- Yahoooligans</li> <li>- CBBC Search</li> <li>- Kidsclick</li> </ul>
Exchanging information with other pupils and asking questions of experts via e-mail.	<p>Pupils should only use approved e-mail accounts.</p> <p>Pupils should never give out personal information.</p> <p>Consider using systems that provide online moderation e.g. SuperClubs.</p>	<p>SCORE sgfl accounts</p> <p>School Net Global</p> <p>E-mail a children's author</p> <p>E-mail Museums and Galleries</p>
Publishing pupils' work on school and other websites for feedback.	<p>Pupil and parental consent should be sought prior to publication.</p> <p>Pupils' full names and other personal information should be omitted.</p> <p>Pupils should be encouraged to report any inappropriate comments.</p>	<p>SCORE Showcase</p> <p>Making the News</p> <p>Podcasts</p>
Publishing images including photographs of pupils.	<p>Parental consent for publication of photographs should be sought.</p> <p>Photographs should not enable individual pupils to be identified.</p> <p>File names should not refer to the pupil by name.</p>	<p>Making the News</p> <p>SuperClubs</p> <p>Learninggrids</p> <p>Museum sites, etc.</p> <p>Digital Storytelling</p> <p>BBC – Primary Art</p>
Communicating ideas within blogs, chat rooms or online forums.	<p>Only blogs/chat rooms dedicated to educational use and that are moderated should be used.</p> <p>Access to other social networking sites should be blocked.</p> <p>Pupils should never give out personal information.</p>	<p>SCORE Blogs</p> <p>SuperClubs</p> <p>Skype</p> <p>FlashMeeting</p> <p>VLE</p>
Audio and video conferencing to gather information and share pupils' work.	<p>Pupils should be supervised.</p> <p>Only sites that are secure and need to be accessed using an e-mail address or protected password should be used.</p>	<p>Skype</p> <p>FlashMeeting</p> <p>National Archives "On-Line"</p> <p>Global Leap</p> <p>National History Museum</p> <p>Imperial War Museum</p>