SMART VISION SCHOOL

E-SAFETY POLICY

Rationale

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. Currently the internet technologies children and young people are using both inside and outside of the classroom include:

- Websites
- Learning Platforms (MLE) and Virtual Learning Environments
- Email and Instant Messaging
- Chat Rooms and Social Networking
- Blogs
- Podcasting
- Video Broadcasting
- Downloading from the internet
- Gaming
- Mobile/Smart phones with text, video and/or web functionality
- Other mobile devices with web functionality

Scope

This policy applies to all pupils, all teaching staff, all support staff, all governors and all volunteers.

Aim

At Smart Vision School we understand the responsibility to educate our pupils in e-Safety issues; teaching them the appropriate behaviors and critical thinking to enable them to remain both safe and legal when using the internet and related technologies, in and beyond the context of the classroom.

This policy recognizes our commitment to keeping children safe and acknowledges its part in the school's overall Safeguarding policies and procedures. It shows our commitment to meeting the requirements to keep pupils safe and operate in conjunction with other policies and procedures.

Managing Internet Access:

- All staff, volunteers and students must read and sign the 'Acceptable Use of Technology' policy annually and any new staff before using any school ICT resource.
- Parents will be informed that pupils will be provided with supervised Internet access.
- E-Safety rule Posters will be displayed in classrooms – appropriate to the Key Stage.
- If staff or pupils discover unsuitable sites, the URL (address), time, content must be reported to IT Department to block the site.
- All children must understand that if they see an unacceptable image on a computer screen, they must lower the screen (laptop) or turn off the screen, and then report immediately to a member of staff.
- School will ensure that the use of Internet derived materials by pupils and staff complies with copyright law.
- Pupils will be taught how to be SMART online and if using the Internet in school will be given clear objectives for its use.
- Pupils will be taught to be critically aware of the materials they are shown and how to validate information before accepting its accuracy.

- Children will be taught about the risk of Online Bullying, how to avoid it and what to do if it happens, during lessons on ICT Safety. Please refer to our Cyberbullying policy.
- The School's filters will block sites which are deemed to contain inappropriate material or content.

Online Communication and Social Networking (Parents and Pupils):

- Pupils may only use approved e-mail accounts in school, as part of curriculum teaching, which will be deactivated upon leaving.
- Pupils will be taught to use e-mail accounts safely and appropriately in order to prevent exposure to offensive or inappropriate e-mails.
- Pupils will be taught to treat incoming e-mails as suspicious and not to open attachments unless the author is known.
- Access in school to external personal e-mail accounts will be allowed for staff only.
- Pupils will be taught not to reveal personal details of themselves or others, including that which may identify them or their location, in any online communication – email, social networking or otherwise.
- Pupils will be advised about the possible consequences of placing personal photos on any social network space.
- Pupils will be advised of the dangers of meeting anyone from online communications and the importance of how to report concerns to a safe adult.
- Pupils and parents will be advised that the use of social network spaces outside school brings a range of dangers for primary aged pupils and only moderated social networking sites should be used for this age range.
- Children will be educated about the dangers of social media and empowered with the skills to protect themselves online, to prevent adverse consequences.
- Parents will be requested to adhere to the 'Parental Code of Conduct'.

Staff Guidance on the use of Social Networking and Professional Conduct Online:

- It is never acceptable to accept a friendship request from a child from the school as in almost all cases children of primary age using such networks will be breaching the terms and conditions of use of those networks. It is also extremely inadvisable to accept as friends' ex-pupils who are still minors.
- Staff who wish to engage with social media sites, such as Facebook, Twitter or Instagram etc, should be aware that they are representatives of the school and they should not engage with or post comments which affect the professional identify of the school or can be considered inappropriate in nature or defamatory in nature.
- Staff are required to follow these guidelines and demonstrate acceptable conduct at all times when using the school's IT systems and also act in a professional manner when accessing the internet from home. The school and Local Authority will be informed in the case of misuse or unprofessional conduct.
- Staff may only take photos in school, for school use, on school provided ipads or technology and not on personal devices.
- Any images of children within the school that are posted on the website or blog, will have the required parental permission.

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 are not allowed to be used by pupils in school and staff are aware that they will not be used for personal use during lessons or formal school time, unless during emergencies. The sending of abusive or inappropriate text messages, files by Bluetooth or any other means is forbidden.
- Staff should use a school phone where contact with parents is required.
- Any device which may capture or record an image, or connect to the internet, belonging to a pupil, must be left in the school office.

Information System Security:

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

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. Neither the school nor ISP can accept liability for the material accessed, or any consequences of Internet access.
- The school will audit ICT use to establish if the policy is adequate, effective or in need of modification and that the implementation of the 'Safeguarding Children and Young People in the Context of Technology and Social Media (E-SAFETY)' policy is appropriate.

Use of ICT Equipment :

The computer system is owned by the school. "The computer system" means all computers and associated equipment belonging to the school, whether part of the school's integrated network or stand-alone, or taken offsite. The school provides portable ICT equipment such as ipads, laptop computers, voice recorders, video cameras and digital cameras to enhance the children's education and to allow staff to make efficient use of such equipment to enhance their own professional activities.

- The school reserves the right to examine or delete any files that may be held on its computer systems and to monitor any Internet sites visited.
- If an individual leaves the employment of the school, any equipment, e.g. laptops, iPads, cameras etc must be returned;

Handling e-safety Complaints:

- Complaints of Internet misuse will be dealt with by the IT Integrator.
- Any complaint about staff misuse must be referred to the Head of Dept/Principal.
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures and policy.
- Any instance will be managed appropriately with due regard to confidentiality.

Appendix A

Useful resources for teachers

Common Sense
www.commonsense.org

Think U Know
www.thinkuknow.co.uk

Child Exploitation and Online Protection Centre
www.ceop.gov.uk

Childnet
www.childnet-int.org

Digizen
www.digizen.org

Kidsmart
www.kidsmart.org.uk

Useful resources for parents

Common Sense for Parents
www.commonsensemedia.org

Family Online Safe Institute
www.fosi.org

Internet Watch Foundation
www.iwf.org.uk

This list is not exhaustive and more resources can be found on the school website.