# E-SAFETY POLICY

# VANTAGE ACADEMY TRUST

Date approved: 30th January 2023
*Date for revision: January 2024
Responsibility: LGB
Approved by the LGB

Signature of Chair of Directors ______________________________
*subject to any relevant changes in legislation or other appropriate guideline

**SS Simon & Jude Church of England Academy Trust**, (A Company Limited by Guarantee), Registered in England & Wales, Registered address, Newport Road, Bolton, BL3 2DT, Company Number: - 08240918

Our e-Safety Policy has been written by the school, building on the London Grid for Learning (LGfL) exemplar policy and Becta guidance.

## CONTEXT

*Harnessing Technology: Transforming learning and children's services* [1] sets out the government plans for taking a strategic approach to the future development of ICT.

*"The Internet and related technologies are powerful tools, which open up new prospects for communication and collaboration. Education is embracing these new technologies as they bring with them fresh opportunities for both teachers and learners.*

*To use these technologies effectively requires an awareness of the benefits and risks, the development of new skills, and an understanding of their appropriate and effective use both in and outside of the classroom."* DfES, eStrategy 2005

The Green Paper *Every Child Matters*[2] and the provisions of the *Children Act 2004*[3], *Working Together to Safeguard Children*[4] sets out how organisations and individuals should work together to safeguard and promote the welfare of children.

The 'staying safe' outcome includes aims that children and young people are:

- safe from maltreatment, neglect, violence and sexual exploitation
- safe from accidental injury and death
- safe from bullying and discrimination
- safe from crime and anti-social behaviour in and out of school

1. http://www.dfes.gov.uk/publications/e-strategy/
2. See The Children Act 2004 [http://www.opsi.gov.uk/acts/acts2004/20040031.htm]
3. See Every Child Matters website [http://www.everychildmatters.gov.uk]
4. Full title: Working Together to Safeguard Children: A guide to inter-agency working to safeguard and promote the welfare of children. See Every Child Matters website [http://www.everychildmatters.gov.uk/_files/AE53C8F9D7AEB1B23E4035 14A6C1B17D.pdf]

- secure, stable and cared for.

Much of these aims apply equally to the 'virtual world' that children and young people will encounter whenever they use ICT in its various forms. For example, we know that the internet has been used for grooming children and young people with the ultimate aim of exploiting them sexually; we know that ICT can offer new weapons for bullies, who may torment their victims via websites or text messages; and we know that children and young people have been exposed to inappropriate content when online, which can sometimes lead to their involvement in crime and anti-social behaviour.

It is the duty of the school to ensure that every child in their care is safe, and the same principles should apply to the 'virtual' or digital world as would be applied to the school's physical buildings.

This Policy document is drawn up to protect all parties – the students, the staff and the school and aims to provide clear advice and guidance on how to minimise risks and how to deal with any infringements.

## THE TECHNOLOGIES

ICT in the 21st Century has an all-encompassing role within the lives of children and adults. New technologies are enhancing communication and the sharing of information. Current and emerging technologies used in school and, more importantly in many cases, used outside of school by children include:

- The Internet
- School learning platform including use of wikis, forums and e-portfolios
- e-mail
- Instant messaging (http://www.msn.com, http://info.aol.co.uk/aim/) often using simple web cams
- Blogs (an on-line interactive diary)
- Podcasting (radio / audio broadcasts downloaded to computer or MP3/4 player)
- Social networking sites (Popular www.myspace.com / www.piczo.com / www.bebo.com / http://www.hi5.com / www.facebook.com, www.twitter.com)
- Video broadcasting sites (Popular: http://www.youtube.com/, tiktok)
- Chat Rooms (Popular www.teenchat.com, www.habbohotel.co.uk)
- Gaming Sites (Popular www.neopets.com, http://www.miniclip.com/games/en/, http://www.runescape.com/)
- Music download sites (Popular http://www.apple.com/itunes/ http://www.napster.co.uk/ http://www-kazzaa.com/, http://www-livewire.com/)
- Mobile phones with camera and video functionality
- Smart phones with e-mail, web functionality and cut down 'Office' applications.

## 2. WHOLE SCHOOL APPROACH TO THE SAFE USE OF ICT

Creating a safe ICT learning environment includes three main elements at ST JAMES:

- An effective range of technological tools;
- Policies and procedures, with clear roles and responsibilities;
- A comprehensive e-Safety education programme for pupils, staff and parents.

*Reference: Becta - E-safety Developing whole-school policies to support effective practice* [5]

## 3. ROLES AND RESPONSIBILITIES

e-Safety is recognised as an essential aspect of strategic leadership in this school and the Head, with the support of Governors, aims to embed safe practices into the culture of the school. With the support of the ICT Co-ordinator the Principal ensures that the Policy is implemented and compliance with the Policy is monitored. The ultimate responsibility for e-Safety has been designated to Nicola Watson (ICT Subject Leader).

Our e-Safety Coordinator ensures they keep up to date with e-Safety issues and guidance through liaison with the Local Authority e-Safety Officer and through organisations such as Becta and The Child Exploitation and Online Protection (CEOP)[6]. The school's e-Safety coordinator ensures the Head, senior management and Governors are updated as necessary.

All teachers are responsible for promoting and supporting safe behaviours in their classrooms and following school e-Safety procedures.

All staff should be familiar with the schools' e-Safety Policy including:

- Safe use of e-mail;
- Safe use of Internet including use of internet-based communication services, such as instant messaging and social network;
- Safe use of school network, equipment and data;
- Safe use of digital images and digital technologies, such as mobile phones and digital cameras;
- publication of pupil information/photographs;
- eBullying / Cyberbullying procedures;
- their role in providing e-Safety education for pupils;

Staff are reminded / updated about e-Safety matters at least once a year and the school dedicates one day per year to follow the National E-Safety Day.

[5] http://schools.becta.org.uk/index.php?section=is

[6] http://www.ceop.gov.uk/

## 4. TEACHING AND LEARNING

**Internet use will enhance learning:**

- The school Internet access will be designed expressly for pupil use and will include filtering appropriate to the age of pupils.
- Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.
- 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 school will ensure that the use of Internet derived materials by staff and pupils complies with copyright law.
- Pupils should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

## 5. MANAGING INTERNET ACCESS

**Information system security:**

- School ICT systems security will be reviewed regularly.
- Virus protection will be updated regularly.
- Security strategies will be discussed with the Local Authority.

**E-mail:**

- Pupils may only use approved e-mail accounts on the school system.
- Pupils must immediately tell a teacher if they receive offensive e-mail.
- In e-mail communication, pupils must not reveal their personal details or those of others, or arrange to meet anyone without specific permission.
- Incoming e-mail should be treated as suspicious and attachments not opened unless the author is known.
- The school should consider how e-mail from pupils to external bodies is presented and controlled.
- The forwarding of chain letters is not permitted.

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

- Staff or pupil personal contact information will not generally be published. The contact details given online should be the school office.

**Social networking and personal publishing:**

- The school will control access to social networking sites, and consider how to educate pupils in their safe use.

- 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, their friends or their location.

- Pupils and parents will be advised that the use of social network spaces outside school brings a range of dangers for primary aged pupils

- Homophobic, biphobic and transphobic language and online bullying both on school computers and outside of school will not be tolerated and that the same sanctions apply to online homophobic, biphobic and transphobic bullying as in the classroom.

**Managing filtering:**

- The school will work with the LA to ensure that systems to protect pupils are reviewed and improved.

- If staff or pupils come across unsuitable on-line materials, the site must be reported to the e-Safety Coordinator.

**Managing videoconferencing & webcam use:**

- Videoconferencing should use the educational broadband network to ensure quality of service and security.

- Pupils must ask permission from the supervising teacher before making or answering a videoconference call.

- Videoconferencing and webcam use will be appropriately supervised for the pupils' age.

**Protecting personal data:**

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

**Assessing risks:**

- The school will take all reasonable precautions to prevent access to inappropriate 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 a computer connected to the school network. Neither the school nor Bolton LA can accept liability for any material accessed, or any consequences of Internet access.

- The school should audit ICT use to establish if the e-safety policy is adequate and that the implementation of the e-safety policy is appropriate and effective.

**Community use of the Internet:**

- The school will liaise with local organisations to establish a common approach to e-safety.
- The school will be sensitive to internet related issues experienced by pupils out of school, e.g. social networking sites, and offer appropriate advice.
- Community use of the Internet:
- The school will liaise with local organisations to establish a common approach to e-safety.
- The school will be sensitive to internet related issues experienced by pupils out of school, e.g. social networking sites, and offer appropriate advice.

## 7. COMMUNICATION OF THE E-SAFETY POLICY

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

- e-Safety rules will be posted in all rooms where computers are used and discussed with pupils regularly.
- Pupils will be informed that network and Internet use will be monitored and appropriately followed up.
- Children are also taught about cyber-bullying via assemblies

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

- All staff will be given the School e-Safety Policy and its importance explained.
- Staff must be informed that network and Internet traffic can be monitored and traced to the individual user.
- Staff that manage filtering systems or monitor ICT use will be supervised by senior management and work to clear procedures for reporting issues.
- Staff must be aware that it is not safe to search using Google Images as this option does not always filter inappropriate images effectively. Children are to be taught to search for images using Google 'Web' search and to consider whether website would be suitable.

**Enlisting parents' and carers' support:**

- The school will ask all new parents to sign the parent/pupil agreement when they register their child with the school. This is to be reviewed annually by the ICT Co-ordinator.

## 8. HOW WILL COMPLAINTS REGARDING E-SAFETY BE HANDLED?

The school will take all reasonable precautions to ensure e-Safety. However, owing to the international scale and linked nature of Internet content, the availability of mobile technologies and speed of change, it is not possible to guarantee that unsuitable material will never appear on a school computer or mobile device. Neither the school nor the Local Authority can accept liability for material accessed, or any consequences of Internet access.

- Complaints of internet misuse will be dealt with by a senior member of staff.
- Any complaint about staff misuse must be referred directly to the Principal.
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.
- Pupils and parents will be informed of consequences for pupils misusing the Internet.

Staff and pupils are given information about infringements in use and possible sanctions. Sanctions available include:

- interview/counselling by Class Teacher/e-Safety Coordinator/Principal;
- informing parents or carers;
- removal of Internet or computer access for a period, [which could ultimately prevent access to files held on the system];
- removal of access to the school's learning platform for a period;
- referral to LA/Police.

Our e-Safety Coordinator acts as first point of contact for any complaint. Any complaint about staff misuse is to be referred directly to the Principal.

Complaints of cyberbullying are dealt with in accordance with this policy and our Anti-Bullying Policy. Complaints related to child protection are dealt with in accordance with this policy and protection procedures as detailed in the Child Protection Policy.

Procedures for the safeguarding of data and information are also detailed in both Data Protection and Information Handling and Information Management policies respectively.

Adopted by the Governing Body: January 2023

To be reviewed on: January 2024