St Jude's Church of England Primary Academy

E-Safety Policy

2018-19

St Jude's C of E Academy

E-Safety

Introduction

1.1. E-Safety encompasses Internet technologies and electronic communications such as mobile phones and wireless technology. Most children are enthusiastic Internet users - particularly of interactive services like: Email, Chat and Instant Messaging. At St Jude's the education of pupils in e-safety is very important and seen as an essential part of the curriculum and e-safety provision across the school.

1.2. Current and emerging technologies used at St Jude's and, more importantly in many cases, used outside of St Jude's by children include:

- The internet;
- e-mail;
- Instant messaging (www.msn.com) using simple web cams;
- Blogs (an on-line interactive diary);
- Podcasting (radio / audio broadcasts downloaded to computer or MP3/4 player);
- Social networking sites (www.facebook.com);
- Video broadcasting sites (www.youtube.com);
- Chat Rooms (www.teenchat.com);
- Gaming Sites (www.neopets.com);
- Music download sites (www.limewire.com);
- Mobile phones with camera and video functionality;

- Smart phones with e-mail, web functionality and cut down 'Office' applications.

1.3. The New Primary Curriculum states that children should apply their ICT knowledge, skills and understanding confidently and competently in their learning and in everyday contexts and that they become independent and discerning users of technology, recognising opportunities and risks and using strategies to stay safe.

1.4. Across all six areas of learning children learn how to:

- Find and select information from digital and online sources, making judgments about accuracy and reliability;
- Create, manipulate and process information using technology to capture and organise data, in order to investigate patterns and trends;
- Explore options using models and simulations; and combine still and moving images, sounds and text to create multimedia products;
- Collaborate, communicate and share information using connectivity to work with, and present to, people and audiences within and beyond the Academy;
- Refine and improve their work, making full use of the nature and pliability of digital information to explore options and improve outcomes.

E-safety provision at St Jude's will be provided through the following ways:

- A planned e-safety programme as part of computing and PSHE and safeguarding curriculum.
- Key e-safety messages will be reinforced as part of the planned programme of assemblies and class work.
- Pupils will be taught in all lessons to be critically aware of materials/content that they access online and be guided to validate the accuracy of information.
- Pupils should be taught to acknowledge the source of information used and to respect copyright when using material on the internet.
- Staff will sign a code of conduct accepting roles and responsibilities to act as good role models in their own use of ICT, the internet and mobile devices.

Designated person for Child Protection

The Headteacher, Deputy Headteacher, Senior Leaders and all staff are trained in e-safety issues and will be aware of the potential for serious child protection issues to arise from:

- **Sharing of personal data**
- **Access to illegal/inappropriate materials**
- **Inappropriate on-line contact with adults/strangers**
- **Potential or actual incidents of grooming**
- **Cyber-bullying**

Policies and Procedures

1.5. The St Jude's e-safety policy will operate in conjunction with other policies including: Behaviour, Anti-Bullying, Teaching and Learning and Data Protection.

1.6. Our e-Safety Policy has been written building on BECTA government guidance.

1.7. The e-Safety Policy and its implementation will be reviewed annually and where necessary in cases of reported misconduct or risks.

1.8. E-safety will form a key part of the ICT/PSHE Curriculum. Children will be made aware of the dangers and risks of using the Internet and mobile technologies throughout the year. This will include during anti-bullying week, e-safety awareness week and an integral part of ICT lessons.

Internet Access

1.9. The Internet is an essential element of education, business and social interaction. St Jude's has a duty to provide pupils with quality Internet access as part of their learning experience.

1.10. Internet use is a part of our curriculum at St Jude's and a necessary tool for staff and pupils.

1.11. Our Internet access will be designed expressly for pupil use and will use appropriate filtering system.

1.12. Pupils will be taught what internet use is acceptable and what is not and given clear objectives for internet use. Pupils will not use the internet without having permission from a member of staff.

1.13. Pupils will not use social networking sites at school mand will be educated about their safe usage in their own time.

1.14. Pupils will be advised never to give out personal details of any kind, which may identify them, their friends or their location.

1.15. Pupils are forbidden from downloading games or other programs from the Internet.

1.16. The ICT technician will carry out downloading programs from the Internet.

1.17. Public chat-rooms and instant messaging are not allowed and are blocked using the Internet filter.

1.18. Pupils will be educated in 'Information Literacy' and taught how to evaluate the Internet content that they have located. Pupils will be taught the importance of crosschecking information before accepting its accuracy.

1.19. St Jude's will ensure that the use of Internet derived materials by staff and pupils complies with copyright law. Pupils will be taught to reference materials they have found from other sources so as not to infringe copyright or the intellectual property of others.

1.20. Pupils will be taught how to report unpleasant Internet content.

E-mail

1.21. When available, pupils may only use approved e-mail accounts on the school's network. Pupils are not permitted to use their own personal email accounts on Scientia equipment.

1.22. Pupils must immediately tell a teacher if they receive an offensive e-mail.

1.23. In e-mail communications, pupils must not reveal their personal details or those of others, or arrange to meet anyone without specific permission.

1.24. Incoming e-mails should be treated as suspicious and attachments not opened unless the author is known.

1.25. Email sent to an external organisation should be written carefully and authorised before sending, in the same way as a letter written on Scientia headed paper.

1.26. Staff should never use personal e-mail addresses to communicate with pupils. The ICT technician will provide an official school e-mail address for all staff at St Jude's.

Managed Learning Environment

1.27. The MLE is provided for use of staff and pupils only. At present access by any other party is strictly prohibited.

1.28. Pupils should never reveal his/her password to anyone or attempt to access the service using another pupil's login details. Pupils should inform the ICT technician if they feel their password has been compromised.

1.29. All staff and pupils possess a username and password as a level of security. The correct levels of privilege are applied to the correct users.

Published Content and the St Jude's Web site

1.30. Staff or pupil's personal contact information will not be published. The contact details given online should be the office.

1.31. The Headteacher and Deputy Headteacher will take overall editorial responsibility and ensure that content is accurate and appropriate.

1.32. Permission from parents or carers will be obtained before photographs of pupils are published on the web site. Pupils' full names will not be used anywhere on the web site, particularly in association with photographs.

1.33. Work can only be published with the permission of the pupil and parents.

1.34. Pupil image file names will not refer to the pupil by name.

1.35. Pupil image files should be securely stored on the network.

Video Conferencing and Webcam Use

1.36. When available, video conferencing and webcam use will be appropriately supervised.

1.37. Pupils will be taught the dangers of using webcams outside of the school environment.

Portable Devices

1.38. Mobile phones are not to be used at St Jude's; for older children who walk home alone they are to be left at the office at the beginning of each day. The sending of abusive or inappropriate text messages is forbidden.

1.39. Staff should be aware that technologies such as laptops and smartphones may access the Internet by bypassing filtering systems and present a new route to undesirable material and communications.

1.40. All staff are requested to sign a code-of-conduct regarding mobile phones and portable devices and any area where children are present is classed as a 'Mobile Free' Zone.

1.41. Staff should not use their personal mobile phones to contact pupils or capture photographs of children. Alternative equipment will be provided by the school.

1.42. Pupils are taught how to protect themselves from being victims of theft and how to report such an event to the correct authority.

1.43. Any visitors to St Jude's are asked to refrain from any use of portable devices within the school other than the office or staffroom.

Managing Emerging Technologies

1.44. Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use at St Jude's is allowed.

1.45. Technologies such as mobile phones with wireless Internet access can bypass the school's filtering systems and present a new route to undesirable material and communications.

1.46. Games machines including the Sony PlayStation, Microsoft Xbox and others have Internet access, which may not include filtering. These may not be used at St Jude's unless a risk assessment has taken place blocking online use.

Protecting Personal Data

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

Roles and Responsibilities

1.48. Support will be provided by the ICT technician and senior Leadership team. Our computing and e-Safety leader ensures they keep up to date with e-Safety issues and guidance; keeps the Headteacher, senior management and Governors updated as necessary; ensures that any e-safety concerns are reported in the first instance to the e-Safety leader who will investigate the concern and take the appropriate action.

1.49. Our Governors have an understanding of e-Safety issues and strategies at the Academy, and are aware of local and national guidance on e-safety and are updated at least annually on policy developments.

1.50. Our staff have e-safety responsibilities: to be familiar with the policy and to adhere to its' procedures and must be familiar with St Jude's Policy in regard to:

- Safe use of e-mail;
- Safe use of internet;
- Safe use of the 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 and use of the web site;
- E-Bullying / Cyber bullying procedures;
- Their role in providing e-safety education for pupils;
- Staff should be aware that Internet traffic could be monitored and traced to the individual user. Discretion and professional conduct is essential;
- Staff will always use a child friendly, safe search engine when accessing the Internet with pupils. (e.g. Google Safe Search – default settings).

1.51. Academy staff will be reminded/updated about e-safety matters at least once a year.

Managing Internet Access and Other Technologies

1.52. **Information system security**

1.52.1. Academy ICT systems capacity and security will be reviewed regularly.

1.52.2. All staff and pupils possess individual logons and passwords to the Academy network with appropriate access rights and privileges.

1.52.3. Virus protection will be installed on all Academy computers and updated regularly in light of new viruses that weaken the Academy's security.

1.52.4. Staff must ask permission from the e-Safety leader before installing software on any Academy machines, which will be installed by the Network Manager.

1.53. **Managing filtering**

1.53.1. If staff or pupils discover an unsuitable web site, it must be reported to the e-Safety leader or the ICT Technician , the web site can be closed but the computer should not be shut down to allow further investigation.

1.53.2. The ICT technician will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

1.54. **Assessing risks**

1.54.1. St Jude's will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale of linked Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. St Jude's Academy cannot accept liability for the material accessed, or any consequences of internet access.

1.54.2. St Jude's will give responsibility to the ICT technician to monitor the use of Internet, email and messaging services.

1.54.3. St Jude's will audit ICT use to establish if the e-Safety Policy is adequate and that the implementation of the e-Safety Policy is appropriate.

1.55. **Handling e-safety complaints**

1.55.1. Complaints of Internet misuse will be dealt with by the e-Safety leader and Deputy Headteacher

1.55.2. Any complaint about staff misuse must be referred to the Headteacher;

1.55.3. Complaints of a Safeguarding nature must be dealt with in accordance with St Jude's Safeguarding and Child Protection policies and procedures

1.55.4. Pupils and parents will be informed of the complaints procedure.

1.56. **Enlisting parents' support**

1.56.1. The e-Safety Policy will be available from the office on request and on the school web site.

1.56.2. Parents will be encouraged and supported to monitor their children's use of technology at home.

1.56.3. The Academy will provide e-safety sessions for parents and links such as CEOP are provided via the school website.

This policy will be reviewed annually:Review date: July 2019

Annex 1 – E-Safety Glossary

The definitions used in the E-Safety Policy are:

Avatar: A graphic identity selected by a user to represent him/herself to the other parties in a chat-room or when using instant messaging.

Becta: The Government's lead partner in the strategic development and delivery of its

e-strategy from 1998-2011.

Chat-room: An area on the Internet or other computer network where users can communicate in real time, often about a specific topic.

Filtering: A method used to prevent or block users' access to unsuitable material on the Internet.

Information Literacy: The ability to locate pertinent information, evaluate its reliability, analyse and synthesise it to construct personal meaning and apply it to informed decision making.

Instant messaging (IM): A type of communications service that enables you to create a kind of private chat room with another individual in order to communicate in real time over the Internet, analogous to a telephone conversation but using text-based, not voice-based, communication.

Peer-to-peer (P2P): A peer-to-peer network allows other users to directly access files and folders on each other's computer. File sharing networks such as 'Lime Wire' creates weaknesses in networks security by allowing outside users access to the schools resources.

Spam: Unsolicited junk email. The term is also used to describe junk text messages received via mobile phones. A related term, spim (or spIM), describes receiving spam via instant messaging.

Spoofing: Assuming the identity of someone else, using an email address either guessed or harvested from repositories of valid email addresses (such as the address book of a virus-infected computer). Spoofing is typically practised to veil the source of virus-laden emails or, often, to obtain sensitive information from spam recipients, without revealing the source of the spammer.

Trojan Horses: A virus, which infects a computer by masquerading as a normal program. The program contains additional features added with malicious intent. Trojan horses have been known to activate webcams, for example, without the knowledge of the PC user.

Video Conferencing: The process of conducting a conference between two or more participants over a network, involving audio and often text as well as video.

Virus: A computer program that enters a computer, often via email, and carries out a malicious act. A virus in a computer can corrupt or wipe all information in the hard drive, including the system software. All users are advised to guard against this by installing anti-virus software.

Webcam: A webcam is a camera connected to a computer that is connected to the Internet. A live picture is uploaded to a website from the camera at regular intervals, typically every few minutes. By looking at the website you can see what the camera sees – almost as it happens.