St. Anne's E-Safety Policy 2017-18

Introductory Statement

The internet and communication technology resources provide powerful tools to open up new opportunities for all ages.

At St. Anne's we aim to provide our pupils, staff and the community access to the internet and new emerging technologies to enhance our curriculum and encourage 'digital literacy' in all.

We aim to include communication technologies in all area of the curriculum to ensure all children are equipped with the necessary skills needed for the future. In doing this we aim to raise educational standards across the curriculum, promote pupil achievement, support professional development of staff and enhance the school's management of information and business administration systems.

While St. Anne's encourages and promotes the use of communication technology we are aware of the associated dangers of the internet and other emerging technologies, such as,

- Children might inadvertently access content of an unsavoury, distressing or offensive nature on the internet or receive inappropriate or distasteful emails
- Children might receive unwanted or inappropriate messages from unknown senders via email or via files sent by Bluetooth. They might also be exposed to abuse, harassment, or 'cyber bullying' via email, text or instant messaging, in chat rooms or on social-networking websites
- Chat rooms provide cover for unscrupulous individuals to groom children

We also understand how such issues are publicised and highlighted by today's media with an ever increasing society reliant on information communication technology.

It is agreed by the government, governing body of our school and staff, that the risks associated with such technologies, such as the internet, is far outweighed by the benefits and enrichment these technologies provide to our children's lives.

- The internet provides instant access to a wealth of up-to-the minute information and resources from across the world, which would not ordinarily be available.
- Use of email, mobile phones, Internet messaging and blogs all enable improved communication and facilitate the sharing of data and resources.
- Virtual Learning Environments (VLE's) provide children with a platform for personalised and independent learning.
- The internet helps to improve children's reading and research skills.

.

Procedures for use of a shared network

At St. Anne's, a shared cable and wireless network is accessible from all classrooms. This network links and saves information onto a central server located in the IT suite. The network is regulated and maintained by the ICT coordinator, Headteacher and Office Administrator and overseen technically by Clear Two.

St Anne's is responsible to ensure:

- Users are given their own login and passwords for the school network, including all staff, each year group and guest users.
- These must not be disclosed or shared.
- The ICT coordinator will be allowed to obtain copies of all passwords but these must be kept in a secure area of the school.
- The ICT coordinator/Clear Two/Headteacher will be authorised by the school governing body to carry out routine checks of all users' accounts and files, in the interest of child safety.
- Users are aware of the procedures and sanctions imposed by this policy with regards to the school network.
- The wireless technology will be encrypted to prevent outsiders being able to access it.

Users are responsible to ensure

- Users access the school network using their own login and password.
- Users must respect confidentiality and attempts should not be made to access another individual's personal folder on the network without permission.
- Software should not be installed, nor programmes downloaded from the internet without prior permission from the network manager (Clear Two)
- Removable media (e.g. encrypted pen drives/memory sticks, CD-ROMs) must be scanned for viruses before being used on a machine connected to the network.
- Machines must never be left 'logged on' and unattended. If a machine is to be left for a short while, it must be 'locked.' (Ctrl+alt+del followed by 'lock computer').
- Machines must be 'logged off' correctly after use.
- Any data about children must be stored on encrypted pen drives if it is to be taken off the school premises.
- Staff laptops do not contain any data about children unless they are password protected.

Procedures for Use of the Internet and Email

- All users, including community users, must sign an 'Acceptable use Agreement' before access to the internet and email is permitted in the school (March 2017)

- Parent or carer consent is needed by school for children to be allowed to access to the internet or email (March 2017)
- Users must access the Internet and email using their own logon/password and not those of another individual.
- Passwords must remain confidential and no attempt should be made to access another user's email account.
- Headteacher will be allowed to obtain copies of all passwords but these must be kept in a secure area of the school and only consulted with the authority of the user.
- The internet and email must only be used for professional or educational purposes.
- Children must be supervised at all times when using the internet and email.
- Procedures for safe internet use and sanctions will be clearly displayed in the ICT suite and throughout the school.
- Children will not be allowed to carry out any search on a search engine which has not been checked by a responsible adult.
- Accidental access to inappropriate, abusive or racist material is to be reported without delay to the DP (Headteacher/deputy)and Clear Two, and a note of the offending website address (URL) taken so that it can be blocked.
- Internet and email filtering software is installed to restrict access, as far as possible, to inappropriate or offensive content and to reduce the receipt of 'spam,' junk or unwanted correspondence. This is to be reviewed and updated regularly by Clear Two
- Internet and email use will be monitored regularly in accordance with the DATA PROTECTION ACT.
- Email addresses will not be assigned to individual children and if children are assigned a group email for educational purposes, it will not be in a form which makes them easily identifiable to others.
- Users must not disclose any information of a personal nature or in reference to the school in an email or on the Internet. This includes mobile and home phone numbers, addresses, or anything else which might allow them to be identified. If such information is needed the Headteacher/ICT coordinator must be consulted.
- All emails sent should be courteous and the formality and tone of the language used appropriate to the reader. No strong or racist language will be tolerated. Sanctions appropriate to the case will be imposed on any users who break this code.
- Bullying, harassment or abuse of any kind via email will not be tolerated. Sanctions appropriate to the case will be imposed on any users who break this code.
- If users are bullied, or offensive emails are received, this must be reported immediately to a trusted adult or member of staff within the school. Emails received should not be deleted, but kept for investigation purposes.

- Anti virus software is used on all machines and this is regularly updated to ensure it's effectiveness (overseen by Clear Two)
- All email attachments must first be scanned before they can be opened.
- Users must seek permission before downloading any files from the internet.
- All users will be made aware of copyright law and will acknowledge the source of any text, information or image copied from the internet.

Procedures for Use of Instant Messaging (IM), Chat and Weblogs

At St. Anne's it has been agreed that access to the following will be banned across the school, as such resources are considered not age appropriate for children at St. Anne's. In light of this all staff will also be denied access to these resources.

- The use of Instant Messaging (e.g. MSN messenger) and hotmail is not permitted. All staff will be provided with a school email address.
- Use of social networking websites, such as Bebo, My Space, Facebook, Habbo, etc. are not permitted.
- Children and staff must not access public or unregulated chat rooms.

These resources are not accessible through any login in the school to ensure children's safety.

- Use of weblogs is permitted. This will be supervised and children will be reminded of the safe practices and behaviours to adopt when posting material, as well as the need to adopt a formal and polite tone at all times.

Procedures for Use of Cameras, Video Equipment and Webcams

- Permission must be obtained from a child's parents or carer before photographs or video footage can be taken. (permission forms sent out 22.2.17)
- Photographs or video footage will be downloaded immediately and saved into a designated folder. This will be 'password protected' and accessible only to authorised members of staff.
- Staff should not use their own camera, video recorder or camera phone during a trip or visit. Staff are provided with school I pads and a school registered I phone for off-site visits.
- Children should not accept files sent via Bluetooth to their mobile phones by an unknown individual. If they do, and the content received is upsetting or makes them feel uncomfortable, they should pass this on to a trusted adult straight away.
- Video conferencing equipment and webcams must be switched off (disconnected) when not in use.
- Webcams must not be used for personal communication and should only be used with an adult present.

- Children and staff must conduct themselves in a polite and respectful manner when representing the school in a video conference or when corresponding via a webcam. The tone and formality of the language used must be appropriate to the audience and situation.

Procedures to ensure safety of the school's website

- The Headteacher/SMT are the designated members of staff who is responsible for approving all content and images to be uploaded onto its website prior to it being published.
- The school's website should be subject to frequent checks by the ICT coordinator to ensure that no material has been inadvertently posted, which might put children or staff at risk.
- Copyright and intellectual property rights must be respected.
- Full names must not be used to identify individuals portrayed in images uploaded onto the school website. Similarly, if a child or member of staff is mentioned on the website, photographs which might enable this individual to be identified must not appear.
- Images of individual children will not be posted on the school website. Only group photographs will be used.
- When photographs to be used on the website are saved, names of individuals portrayed therein should not be used in file names.
- If the school website contains a Guestbook, public noticeboard, forums or weblogs, these must be monitored regularly to check that no personal information or inappropriate or offensive material has been posted.

Procedures for using mobile phones and Personal Digital Assistants (PDAs)

Children's use of mobile phones is banned. If children have a mobile phone in their possession they must give it to an adult for safe keeping in a secure area. If children are caught using mobile phones they will have the phone confiscated until the end of the school day, when a parent or carer will be asked to collect the phone. If the offence is committed repeatedly, further action will be taken by the school.

- If children/staff receive unwanted, inappropriate, unsavoury or hurtful calls, text messages or files sent via Bluetooth out of school, they should report these messages to the Headteacher.
- Children will be made aware of these procedures and encouraged not to accept unknown messages or give personal details such as mobile numbers to unknown persons.

Procedures for using wireless games consoles

Wireless games consoles will be banned at all times. If children have such items in their possession they must give it to an adult for safe keeping in a secure area. If children are caught using such items they will have the item confiscated until the end of the school day, when a parent or carer will be asked to collect the item. If the offence is committed repeatedly further action will be taken by the school.

Procedures for using portable media players (e.g. iPods)

Personal Portable media players will be banned at all times. If children have portable media players in their possession they must give it to an adult for safe keeping in a secure area. If children are caught using portable media players they will have the item confiscated until the end of the school day, where a parent or carer will be asked to collect the item. If the offense is committed repeatedly further action will be taken by the school.

Sanctions to be imposed if procedures are not followed

The headteacher is responsible for dealing with incidents in which procedures are not adhered to. Sanctions which may be imposed are;

- Letters may be sent home to parents or carers (if applicable).
- Users may be suspended from using the school's computers, Internet or email, etc. for a given period of time/ indefinitely.
- Details may be passed on to the police in more serious cases.
- Legal action may be taken in extreme circumstances.

The sanctions imposed will be considered on an individual basis by the Headteacher in any case of misuse.

Cyberbullying

Cyberbullying is the use of information and communication technology, particularly mobile phones and the internet, deliberately to upset someone else.

- If children experience such behaviour by others they should report it to a member of staff immediately.
- If such incidents are reported to staff, they should take action in line with St. Anne's anti-bullying policy.
- Parent workshops will be held annually to warn parents of the dangers of underage access of social media sites and potential cyber bullying.

- Newsletters and the school website will contain links for parents who are concerned about internet safety.

Parental Support

Internet use in pupils' homes is increasing rapidly, encouraged by low cost access and developments in mobile technology. Unless parents are aware of the dangers, pupils may have unrestricted and unsupervised access to the Internet in the home. The school may be able to help parents plan appropriate, supervised use of the Internet at home and educate them about the risks. Parents should also be advised to check whether their child's use elsewhere in the community is appropriate.

- Parents' attention will be drawn to the school e–Safety Policy in newsletters, the school prospectus and on the school website.
- A partnership approach to e-Safety at home and at school with parents will be encouraged. This may include offering advice at parent evenings, through workshops and demonstrations.
- Parents will be encouraged to read and sign the school Acceptable Use Policy for pupils and discuss its implications with their children.
- Interested parents will be referred to organisations listed in the "e–Safety contacts section

Radicalisation and Extremism

The school's safeguarding and PREVENT policies which are available on our website and in school, covers Radicalisation and Extremism.

1. Radicalisation refers to the process by which a person comes to support terrorism and forms of extremism leading to terrorism.

2. Extremism is defined by the Government in the Prevent Strategy as: Vocal or active opposition to fundamental British values, including democracy, the rule of law, individual liberty and mutual respect and tolerance of different faiths and beliefs. We also include in our definition of extremism calls for the death of members of our armed forces, whether in this country or overseas.

3. Extremism is defined by the Crown Prosecution Service as: The demonstration of unacceptable behaviour by using any means or medium to express views which:

- Encourage, justify or glorify terrorist violence in furtherance of particular beliefs.
- Seek to provoke others to terrorist acts.
- Encourage other serious criminal activity or seek to provoke others to serious criminal acts.
- Foster hatred which might lead to inter-community violence in the UK.

4. There is no such thing as a "typical extremist": those who become involved in extremist actions come from a range of backgrounds and experiences, and most individuals, even those who hold radical views, do not become involved in violent extremist activity.

5. Pupils may become susceptible to radicalisation through a range of social, personal and environmental factors - it is known that violent extremists exploit vulnerabilities in individuals to drive a wedge between them and their families and communities. It is vital that school staff are able to recognise those vulnerabilities.

6. Indicators of vulnerability include:

- Identity Crisis – the student / pupil is distanced from their cultural /religious heritage and experiences discomfort about their place in society.
- Personal Crisis – the student / pupil may be experiencing family tensions; a sense of isolation; and low self-esteem; they may have dissociated from their existing friendship group and become involved with a new and different group of friends; they may be searching for answers to questions about identity, faith and belonging.
- Personal Circumstances – migration; local community tensions; and events affecting the student / pupil's country or region of origin may contribute to a sense of grievance that is triggered by personal experience of racism or discrimination or aspects of Government policy.
- Unmet Aspirations – the student / pupil may have perceptions of injustice; a feeling of failure; rejection of civic life.
- Experiences of Criminality – which may include involvement with criminal groups, imprisonment, and poor resettlement / reintegration.
- Special Educational Need – students / pupils may experience difficulties with social interaction, empathy with others, understanding the consequences of their actions and awareness of the motivations of others.

7. However, this list is not exhaustive, nor does it mean that all young people experiencing the above are at risk of radicalisation for the purposes of violent extremism.

8. More critical risk factors could include:

- Being in contact with extremist recruiters.
- Accessing violent extremist websites, especially those with a social networking element.
- Possessing or accessing violent extremist literature.
- Using extremist narratives and a global ideology to explain personal disadvantage.
- Justifying the use of violence to solve societal issues.
- Joining or seeking to join extremist organisations.
- Significant changes to appearance and / or behaviour.
- Experiencing a high level of social isolation resulting in issues of identity crisis and / or personal crisis.

8.2 Preventing Violent Extremism

Roles and Responsibilities of the Single Point of Contact (SPOC), The SPOC for St Anne's RC Primary is Karen Orrell (Head Teacher), who is responsible for:

- Ensuring that staff of the school are aware that you are the SPOC in relation to protecting students/pupils from radicalisation and involvement in terrorism.
- Maintaining and applying a good understanding of the relevant guidance in relation to preventing students/pupils from becoming involved in terrorism, and protecting them from radicalisation by those who support terrorism or forms of extremism which lead to terrorism.
- Raising awareness about the role and responsibilities of St Anne's RC Primary School School in relation to protecting students/pupils from radicalisation and involvement in terrorism.
- Monitoring the effect in practice of the school's RE curriculum and assembly policy to ensure that they are used to promote community cohesion and tolerance of different faiths and beliefs.
- Raising awareness within the school about the safeguarding processes relating to protecting students/pupils from radicalisation and involvement in terrorism.
- Acting as the first point of contact within the school for case discussions relating to students / pupils who may be at risk of radicalisation or involved in terrorism.
- Collating relevant information from in relation to referrals of vulnerable students / pupils into the Channel* process.
- Attending Channel* meetings as necessary and carrying out any actions as agreed.
- Sharing any relevant additional information in a timely manner.

* Channel is a multi-agency approach to provide support to individuals who are at risk of being drawn into terrorist related activity. It aims to

- Establish an effective multi-agency referral and intervention process to identify vulnerable individuals;
- Safeguard individuals who might be vulnerable to being radicalised, so that they are not at risk of being drawn into terrorist-related activity; and
- Provide early intervention to protect and divert people away from the risks they face and reduce vulnerability

Concluding statement

This policy will be maintained and regularly reviewed by the Headteacher/ICT lead, to ensure that St. Anne's continues to protect children and staff from the dangers of new emerging technologies.

We will ensure all children, staff and school guests are aware of this policy and the procedures associated with this policy.

St. Anne's also states that the sanctions in place for this policy also apply to the use of technologies not stated here that maybe necessary for the education and development of children and staff; for example loaned equipment from CLC and other approved sources.

In addition St. Anne's' states that children and staff will continue to adhere to this policy when using equipment not on site, sanctions and procedures will still apply; for example, authorised trips to the CLC and other approved educational facilities.

We aim to further protect our children, staff and community from the dangers by maintaining and enforcing this E Safety policy.

Policy reviewed February 2017

Approved by Governors:

Next review:

This policy is in accordance with BECTA guidelines, and focuses on the technology resources available at ST. Anne's RC Primary 2016, and outlines the procedures in place to protect users and the sanctions to be imposed if these are not adhered to

E Safety Contacts
CEOP (Child Exploitation and Online Protection Centre): www.ceop.police.uk
Childline: www.childline.org.uk
Childnet: www.childnet.com
Click Clever Click Safe Campaign: http://clickcleverclicksafe.direct.gov.uk
Cybermentors: www.cybermentors.org.uk
Digizen: www.digizen.org.uk
Internet Watch Foundation (IWF): www.iwf.org.uk
Kidsmart: www.kidsmart.org.uk
Teach Today: http://en.teachtoday.eu
Think U Know website: www.thinkuknow.co.uk
Virtual Global Taskforce — Report Abuse: www.virtualglobaltaskforce.com