St Anthony's Catholic Primary School

E-Safety Policy

Written by: Mrs V Berry

Last update: March 2017

Reviewed: March 2017

Adopted by Community Governors – March 2017

School Policy

- The school has computers and Internet access to help learning. On the internet there is a huge wealth of up-to-the minute information and resources from across the world, which would not ordinarily be available. At St Anthony's we believe that the pupils should have opportunity to use these resources to support their learning. Virtual Learning Environments (VLEs) provide children and/or young adults with a platform for personalised and independent learning.

- Children and/or young adults are equipped with skills for the future.
- The Internet provides Instant access to a wealth of up-to-date information and resources from across the world, which would not be otherwise available.
- The Internet helps to improve children's and/or young adults' reading and research skills.
- Email, instant messaging and social networking helps to foster and develop good social and communication skills.

Safety

- The Internet provides access to a greater library of resources to support learning. However, where as the resources in school are carefully selected to be consistent with national and school policies those on the Internet are not. Therefore the school will only connect to the Internet through the Lancsngfl site. A service provider that is monitored and regulated to allow material that has been deemed suitable for children to be viewed. Children will only be allowed to use the Internet when there is adult supervision. The positive use of the internet as a learning resource far outweighs the risks involved. The children will be taught about the issues and concerns and receive ongoing education in choosing and adopting safe practices and behaviours.

Rules for the safe use of the Internet have been established. These rules will be discussed with the pupils and also displayed near Internet access for referral.

Parental approval

- All parents are asked for permission for the acceptance of their child using the school internet service. Attention is drawn to it being a valuable learning aid, and that there are great restrictions to the level of information accessible.

This policy, written in accordance with BECTA guidelines, focuses on the technology available at St Anthony's Catholic Primary and outlines the procedures in place to protect users and the sanctions to be imposed if these are not adhered to.

Adopted by Community Governors – March 2017

Procedures for Use of our Network

- 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 without prior permission from the ICT Co-ordinator.

- Permission to use removable media (e.g. pen drives / memory sticks) must be given by the class teacher.

Procedures for Use of the Internet and Email

- Parental consent is requested to allow internet access in school. All pupils are aware of the Rules for responsible Internet Use.

- The Internet and email must only be used by pupils for educational purposes.

- Children must be supervised at all times when using the Internet and email.

- Procedures for Safe Internet use and sanctions applicable if rules are broken will be clearly displayed

.

- Accidental access to inappropriate, abusive or racist material is to be reported without delay to the E-safety co-ordinator. In the event of access turn **off** the monitor **not** the PC and contact the E-safety co-ordinator who will then make 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.

- Internet and email use will be monitored regularly in accordance with the Data Protection Act.

- Email addresses will not be assigned to individual children.

- Children will be taught the importance of not disclosing any information of a personal nature 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.

- 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 service / establishment. 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 its effectiveness.

- All users will be made aware of Copyright law and will acknowledge the source of any text, information or images copied from the Internet.

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

- The use of Instant messaging (e.g. MSN messenger) is not permitted

- Use of social-networking websites (e.g. Bebo, MySpace, Facebook, Habbo, Piczo, etc.) is not permitted.

- Children/Young adults and staff must not access public or unregulated chat rooms.

Procedures for Use of Cameras, Video Equipment and Webcams

- Permission must be obtained from a child's parent or carer before photographs or video footage can be taken.

- Only school equipment will be used to record images either in school or during a trip or visit. Personal equipment is **not** to be used.

- Children / Young adults 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 straightaway.

- Webcams must not be used for personal communication and should only be used with an adult present.

- Children / Young adults and staff must conduct themselves in a polite and respectful manner when representing the establishment/service 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 website/VLE

- The website administrator/head teacher is responsible for approving all content and images to be uploaded onto its website prior to it being published.
- The school website is subject to frequent checks to ensure that no material has been inadvertently posted, which might put children / young people or staff at risk.
- Copyright and intellectual property rights must be respected.
- Permission will be obtained from parents or carers before any images of children are uploaded onto the School website.
- Names must not be used to identify individuals portrayed in images uploaded onto the School website. Similarly, if a child / young person or member of staff is mentioned on the website, photographs which might enable this individual to be identified must not appear.
- When photographs to be used on the website are saved, names of individuals should not be used as file names.

Procedures for using mobile phones and iPads

- Children in Year 5/6 are permitted to bring in mobile phones however, these are to be kept in a secure location (usually the class teacher's desk) during school hours and only returned at the end of the day.

Sanctions to be imposed if procedures are not followed

- Parents or carers will be informed of any malpractice.
- Users may be suspended from using the school 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.

Concluding Statement

The procedures in this policy will be subject to ongoing review and modification in order to keep up with advances in the technology coming into school and this policy will not remain static. It may be that staff / children might wish to use an emerging technology for which there are currently no procedures in place. It is therefore advisable to state that the use of any emerging technologies will be permitted upon approval by the head teacher and governing body, which will be used to inform future policy updates

Other Policies that have relevance to internet safety

- Safeguarding/Child Protection
- Mobile phone use for staff
- Staff code of conduct