St Anthony's Catholic Primary School

E-Safety Policy

Written by: Mrs V Berry

Updated September 2021

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 in school.

- The Internet provides access to a greater library of resources to support learning. However, whereas 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 BTLancashire 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

- Parental permission is requested yearly to allow all children to use the school internet service.

This policy, written in accordance with BECTA and Lancashire 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.

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.

- Removable media (e.g. pen drives / memory sticks) should not be brought into school unless there has been prior agreement with the headteacher/Computing Co-ordinator. USB drives for memory devices are disabled on classroom and children's desktops PCs.

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.

- 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. Tik Tok, Bebo, MySpace, Facebook, Habbo, Piczo, etc.) is blocked by the BTlancashire Netsweeper and 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

- Parental consent is requested annually 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 can be accessed via Staff devices and must only be used during to access video conferencing meetings via secure channels – SKYPE (LYNC) requests from LCC

email addresses or Teams via Office 365. Zoom video calling may be used in school however this is to be done following the **Zoom Guidelines Document for staff, parents and children** (see appendices). When video calling is used with children additional security measures should be in place (see appendices).

- 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/Twitter pages.

- 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 and Twitter pages are 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 pupils bringing mobile phones into school

We appreciate that children in Year 5/6 may need a mobile phone if they are walking alone to/from school. However, children collected from school do not need a mobile phone as any phone calls which need to be made will be arranged by the relevant member of staff.

As part of our policy we ask for parental permission to be given for children to bring a mobile phone into school. We have phone lockers so that phones can be stored securely away from the

classrooms. All phones must be stored in a locker during the school day and to obtain a locker we will be require a payment of £20 for the cover of key costs.

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

Appendix 1

Introducing Zoom - Parents letter

Safety Advice and Procedures for holding a class 'Zoom' meeting:

We understand how challenging these past few months have been for families and especially for children, and in particular those who have not been able to attend school. Therefore, for our key stage 2 classes, we have decided to hold 'Zoom' meetings, so children have some contact, even if only virtually, with their friends and teachers before the summer holidays.

Next week, you will receive an e-mail from your child's class teacher with information about how the class Zoom meeting will operate as well as the code and password for the meeting. In preparation for this meeting, you'll need to ensure that the device your child uses for this meeting is named as your child's full name- if it isn't they will not be accepted into the meeting. Your child will need to be in a communal room in the house (for example, kitchen, lounge, dining room); be appropriately dressed; it is important that no other member of the family is visible on screen and there is nothing inappropriate or offensive in the background of the screen.

Once all the children have entered, the teacher will lock the meeting so no-one else can join and they will mute the children to briefly discuss the rules. There will be two members of staff present for the duration of the meeting.

Please talk to your child about how to use this app/ website safely and inform them not to share any private or personal information. Ensure your child understands that they should not join any meeting unless they know the host. As always, have regular chats with your child about what they are doing online.

We hope this is something your child can take part in as all teachers are excited to see their classes together again.

Mrs Berry

Appendix 2

Zoom guidance for teachers

Safety Advice and Procedures for holding a class 'Zoom' meeting:

Much of the information below is also mentioned in the 'Safeguarding information for staff' document which contains information lifted from the Lancashire Safeguarding document.
You must read both as some information in each isn't repeated in the other.

- All class Zoom meetings must be on a weekday and between the hours of 9am and 3pm. Friday afternoon would work the best as all children will be at home.
- You may wish to set a time limit- Zoom meetings have a limit of 40 minutes.
- Inform the parents of your class via Groupcall e-mail/Xpressions, with a few days notice at least, that you are going to host the class meeting.
- Within your Groupcall e-mail, send the code and password required to join the meeting. Also inform parents that they'll need to change the name of their device to the child's name otherwise they won't be let into the meeting. Further information to include in the e-mail would be that children must be in a communal room – kitchen, lounge or dining room. They must also be appropriately dressed and must consider that there is nothing inappropriate or offensive in the background of the screen.
- At the beginning of the meeting mute the children and go through some rules about appropriateness of language etc.
- Tell children that they cannot exchange personal data, including handles for computer consoles over this platform.
- Make sure you inform your team leader and Stuart of the date, time and login details for your meeting.
- ALWAYS SET A PASSWORD FOR THE MEETING
- You must host the meeting and you must have a second member of staff present at all times in the meeting.
- Enable the 'waiting room' feature so that you can make sure that there are at least two members of staff in the meeting before you allow any children to join.
- The 'waiting room' will also allow you to see who is wanting to join the meeting.
- Once all children have joined, lock the meeting so no-one else can join.
- Disable the private chat facility so no children can communicate unless with the group.
- You must use a school device, laptop or iPad, and use your school email address.
- If anything inappropriate occurs, end the meeting immediately and inform your team leader straight away.
- Make sure you test that Zoom is working on the device you are using and set up the meeting room at least 15 minutes before the meeting is due to start. Do not however, allow children into the meeting until the official start time. Use the 'end meeting' (maybe called something slightly different) button which will allow you, as the host, to end the meeting for all children at once.

Appendix 3

Further Information

24a. Use of technology for online / virtual teaching

The narrative of section 24 remains relevant. However, there has been a sharp increase in the use of technology for remote learning since March 2020 and this addendum provides some basic guidelines for staff and school leaders.

All settings should review their online safety and acceptable use policies and amend these if necessary, ensuring that all staff involved in virtual teaching or the use of technology to contact pupils are briefed on best practice and any temporary changes to policy / procedures.

When selecting a platform for online / virtual teaching, settings should satisfy themselves that the provider has an appropriate level of security. Wherever possible, staff should use school devices and contact pupils only via the pupil school email address / log in. This ensures that the setting's filtering and monitoring software is enabled.

In deciding whether to provide virtual or online learning for pupils, senior leaders should take into account issues such as accessibility within the family home, the mental health and wellbeing of children, including screen time, the potential for inappropriate behaviour by staff or pupils, staff access to the technology required, etc. Virtual lessons should be timetabled and senior staff, DSL and / or heads of department should be able to drop into any virtual lesson at any time – the online version of entering a classroom.

Staff engaging in online learning should display the same standards of dress and conduct that they would in the real world; they should also role model this to pupils and parents. The following points should be considered: -

- think about the background; photos, artwork, identifying features, mirrors – ideally the backing should be blurred
- staff and pupils should be in living / communal areas – no bedrooms
- staff and pupils should be fully dressed
- filters at a child's home may be set at a threshold which is different to the school
- resources / videos must be age appropriate – the child may not have support immediately to hand at home if they feel distressed or anxious about content

It is the responsibility of the staff member to act as a moderator; raise any issues of suitability (of dress, setting, behaviour) with the child and / or parent immediately and end the online interaction if necessary

Recording lessons does not prevent abuse. If staff wish to record the lesson they are teaching, consideration should be given to data protection issues, e.g., whether parental / pupil consent is needed and retention / storage. If a staff member believes that a child or parent is recording the interaction, the lesson should be brought to an end or that

child should be logged out immediately. Staff, parent and pupil AUPs should clearly state the standards of conduct required.
If staff need to contact a pupil or parent by phone and do not have access to a work phone, they should discuss this with a senior member of staff and, if there is no alternative, always use 'caller withheld' to ensure the pupil / parent is not able to identify the staff member's personal contact details.

This means that senior leaders should:
▪ *review and amend their online safety and acceptable use policies to reflect the current situation*
▪ *ensure that all relevant staff have been briefed and understand the policies and the standards of conduct expected of them*
▪ *have clearly defined operating times for virtual learning*
▪ *consider the impact that virtual teaching may have on children and their parents/ carers / siblings*
▪ *determine whether there are alternatives to virtual teaching in 'real time' – e.g., using audio only, pre-recorded lessons, existing online resources*
▪ *be aware of the virtual learning timetable and ensure they have the capacity to join a range of lessons*
▪ *take into account any advice published by the local authority, MAP or their online safety / monitoring software provider*

This means that staff should:
▪ adhere to their establishment's policy
▪ be fully dressed
▪ *ensure that a senior member of staff is aware that the online lesson / meeting is taking place and for what purpose*
▪ *avoid one to one situations – request that a parent is present in the room for the duration, or ask a colleague or member of SLT to join the session*
▪ *only record a lesson or online meeting with a pupil where this has been agreed with the head teacher or other senior staff, and the pupil and their parent/carer have given explicit written consent to do so*
▪ be able to justify images of pupils in *their possession*

This means that adults should not:
▪ *contact pupils outside the operating times defined by senior leaders*
▪ *take or record images of pupils for their personal use*
▪ *record virtual lessons or meetings using personal equipment (unless agreed and risk assessed by senior staff)*
▪ *engage online while children are in a state of undress or semi-undress*