ST. TERESA'S CATHOLIC PRIMARY SCHOOL

ONLINE SAFETY POLICY

Illuminated by the light of Christ and grounded in love, we grow together, on our journey of discovery and learning.

This Online Safety Policy is part of the School Development Plan and relates to other policies including those for Computing, Anti- Bullying, Child Protection and Safeguarding, PSHE and citizenship.

- Our Online Safety Policy has been written by the school, building on the Lancashire Policy and government guidance. It has been agreed by senior management and approved by governors.
- The Online Safety Policy was revised by: **Mr Hewitt**
- It was approved by the Governors in: **Autumn Term 2018**
- The next review date is: **September 2020**
- All aspects of this policy have been written considering the Keeping children safe in education act 2018 requirements

  'Online safety
  ….*It is essential that children are safeguarded from potentially harmful and inappropriate online material.*'

Managing filtering

'*Governing bodies and proprietors should ensure appropriate filters and appropriate monitoring systems are in place'*

- The school will work with the Lancashire County Council, and Virtue provider to risk assess and individualise the school filtering system so that it is fit for purpose in the context of St Teresa's.
- Any unusual data streams and blocked searches will be monitored by virtue and a report will be sent to the school online safety officer every half term.
- The online safety officer will monitor these reports and analyse blocked material. From this a half termly report will be produced.
- If staff or pupils come across unsuitable on-line materials, the site must be reported to the Online Safety Coordinator, who in turn will ensure that it is blocked by the school filter in future.

Planning for online safety

- The teaching and learning of each unit of computing within the school will begin with an age appropriate online safety lesson following the objectives set out in 'Education for a connected world'.

Why Internet and digital communications are important

- The internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide pupils with quality internet access as part of their learning experience.
- Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils.

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 shown how to publish and present information to a wider audience.

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 will be taught how to report unpleasant internet content e.g. using the CEOP Report Abuse icon or Hector Protector.
- Pupils will be taught about the difference between internet at home and school (filtered) and that google is live.

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 and the provider ,Virtue.

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.
- E-mail accounts for pupils will be deleted when they leave the school.

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.

Publishing pupil's images and work

- Photographs that include pupils will be selected carefully.
- Consider using group photographs rather than full-face photos of individual children.
- Pupils' full names will not be used anywhere on a school Web site or other on-line space, particularly in association with photographs.
- Written permission from parents or guardians as their child starts school is obtained before photographs of pupils are published on the school Web site, outside publications or twitter. This written permission is updated annually by way of a text message to parents requesting that they come in and update the form if needed.
- Work can only be published with the permission of the pupil and parents/guardians
- Parents are clearly informed of the school policy on image taking and publishing, both on school and independent electronic repositories

Social networking and personal publishing

- The school will control access to social networking sites, and consider how to educate pupils and parents 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.
- Pupils will be advised to use nicknames and avatars when using social networking sites.
- Pupils should be advised on security and encouraged to set passwords, to deny access to unknown individuals and to block unwanted communications. Students should only invite known friends and deny access to others.
- Staff will be advised to take precautions when using social networking sites for personal use outside of school.

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 video conference call.
- Video conferencing and webcam use will be appropriately supervised for the pupils' age.

Managing emerging technologies

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.
- The senior leadership team should note that technologies such as mobile phones with wireless Internet access can bypass school filtering systems and present a new route to undesirable material and communications.
- Games machines including the Sony Playstation, Microsoft Xbox and others have Internet access which may not include filtering. Care is required in any use in school or other officially sanctioned location.
- The appropriate use of Learning Platforms will be discussed as the technology becomes available within the school.
- The use of Ipads safely will be explained to the children and parents will be informed on how to put on parent filters.

Protecting personal data

- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 and new GDPR guidelines 2018.

Authorising Internet access

- All staff must read and sign the "Staff Code of Conduct" and "Acceptable Use Policy" before using any school ICT resources, including any laptop issued for professional use.
- The school will maintain a current record of all staff and pupils who are granted access to school 's electronic communications
- Parents will be asked to read the School Acceptable Use Policy for pupil access and discuss it with their child, where appropriate and sign a consent form
- All visitors to the school site who require access to the School network or internet access will be asked to read and sign an Acceptable Use Policy
- Parents will be informed that pupils will be provided with supervised internet access appropriate to their age and ability
- At Key Stage 1 pupils' access to the internet will be by adult demonstration with occasional directly supervised access to specific and approved online materials, which can be located within the school network and has been fully checked by the member of staff

- At Key Stage 2 pupils will be supervised. Pupils will use age-appropriate search engines and online tolls and online activities will be teacher-directed where necessary. Use of the network tools to go to specific websites, rather than searching on search engines is preferred. Children will be regularly reminded of the rules regarding safer internet use.

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 LCC can accept liability for any material accessed, or any consequences of Internet access.
- The school will audit ICT use to establish if the Online Safety policy is adequate and that the implementation of the Online Safety policy is appropriate and effective. This is done on a regular basis using 'online compass'
- The school will ensure monitoring software and appropriate procedures are in place to highlight when action needs to be taken by the school

Responding to Incidents of Concern

- All members of the school community will be informed about the procedure for reporting Online Safety concerns (such as breaches of filtering, cyberbullying, illegal content etc)
- The Online Safety coordinator will record all reported incidents and actions taken in the school Online Safety Incident log and in any other relevant areas eg Bullying or Child Protection log
- The Designated Child Protection Coordinator and other appropriate members of staff will be informed of any Online Safety incidents involving Child Protection concerns, which will then be escalated appropriately.
- The school will manage Online Safety incidents in accordance with the school discipline /behaviour policy where appropriate
- The school will inform parents/guardians of any incidents of concern as and when required
- After any investigations are completed, the school will debrief, identify lessons learned, implement any changes required, and notify the Online Safety group through the governing body.
- Where there is cause for concern or fear that illegal activity which concerns an adult has taken place or is taking place then the school will contact the WSCB LADO and Lancashire County Council HR and OD service so that the incident may be communicated to the Police.
- Where there is cause for concern that a child is at risk of significant harm the school will contact the Central Duty Team

Handling Online Safety complaints

- Complaints of Internet misuse will be dealt with by a senior member of staff.
  Any complaint about staff misuse must be referred to the head teacher. Any staff misuse that suggests a crime has been committed, a child has been harmed or that a member of staff is unsuitable to work with children should be reported to the LADO within one working day in accordance with Lancashire Safeguarding Board policies.
- All members of the school community will need to be aware of the importance of confidentiality and the need to follow the official school procedures for reporting concerns
- Any issues (including sanctions) will be dealt with according to the school's disciplinary, behaviour and Child Protection procedures
- All members of the school community will be reminded about safe and appropriate behaviour online and the importance of not posting any content, comments, images or videos online which cause harm, distress, or offence to any other members of the school community.
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.

How will Cyberbullying be managed?

- Cyberbullying (along with other forms of bullying) of any member of the school community will not be tolerated. See the school Anti bullying Policy and Behaviour Policy
- All incidents of cyberbullying reported to the school will be recorded and investigated Pupils, staff and parents/guardians will be required to work with the school to support the approach to cyberbullying and the school's Online Safety ethos.
- Sanctions for those involve in cyber bullying may include:
- The bully will be asked to remove any material deemed to be inappropriate or offensive
- A service provider may be contacted to remove content if the bully refuses or is unable to delete content.
- Internet access may be suspended at school for the user for a period of time. For other sanction see the school behaviour policy.
- The police will be contacted if a criminal offence is suspected.

How will incidents of sexting will be managed?

What is sexting?

Sexing is ' the production and/or sharing of sexual photos or videos of young people who are under the age of18. It includes nude or nearly nude images and/or sexual acts.

What to do if an incident involving sexting occurs

- Never view download or share the imagery yourself, or ask a child to share or download- This is illegal.
- If you have already viewed the imagery by accident (EG. If a young person has showed it to you before you could ask them not to), report this to the DSL.
- Do not delete the imagery or ask the young person to delete it.
- Do not ask the young person who are involved in the incident to disclose information regarding the imagery. This is the responsibility of the DSL.

- Do not share information about the incident with other staff, the young person it involves or their, or other, parents/carers.
- Do not say or do anything to blame or shame the young people involved.
- Do explain to them that you need to report it and reassure them that they will receive support and help from the DSL.

If a sexting incident comes to your attention, report it to your DSL. The school safeguarding policies will outline codes of practice to be followed.

How will Peer on peer abuse be managed?

- Any staff that are made aware of peer on peer abuse through the use of electronic devices will be reported to a school Designated safeguarding Leader. This leader will follow the anti-bullying policies and procedures to deal with incidents.

How to protect children from online extremism or radicalization

- All members of staff within school will have PREVENT training.
- Members of staff will communicate any concerns regarding extremism or radicalization to the DSL.
- The School online safety officer will monitor blocked searches for signs of extremism or radicalization.

How will Learning Platforms be managed?

- This area will be developed as the Learning Platform in school is introduced
-

How will mobile phones and personal devises be managed?

- The use of mobile phones is covered in the Acceptable Use Policy
- The sending of abusive or inappropriate messages or content via mobile phones or personal devices is forbidden by any member of the school community and any breaches will be dealt with as part of the school behaviour policy
- Mobile phones and personal devices will not be used during lessons or formal school time. Pupils should hand their mobile phone or personal device into the school office at the beginning of the school day and collect it at the end of the day. They should be switched off at all times in line with school policy.
- The Bluetooth function of a mobile phone should be switched off at all times and not be used to send images of files to other mobile phones.
- Electronic devices of all kinds that are brought into school are the responsibility of the user. The school accepts no responsibility for the loss, theft or damage of such items. Nor will the school accept responsibility for any adverse health effects caused by any such devices either potential or actual.

Pupil's use of personal devices

- If a pupil breaches the school policy then the phone or device will be confiscated and will be held in a secure place in the school office. Mobile phones and devices will be released to parents/guardians in accordance with school policy.
- If a pupil need to contact their parent/guardian they will be allowed to use a school phone. Parents are advised not to contact their child via their mobile phone during the school day, but to contact the school office.
- Pupil should protect their phone numbers by only giving them to trusted friends and family members. Pupils will be taught safe and appropriate use of mobile phones and personal devices and will be made aware of boundaries and consequences.

Staff use of personal devices

- Refer to 'Staff code of conduct' policy.
- Mobile phones and devices will be switched off or switched to "silent" mode.
- Bluetooth communication should be "hidden" or switched off and mobile phones or devices will not be used during teaching periods unless permission has been given by a member of the Senior Leadership Team in emergency situations.
- Staff are not permitted to use their own personal phones or devices for contacting children, young people and their families within or outside of the setting in a professional capacity.
- Staff should use a school phone where contact with pupils or parents/guardians is required.
- If members of staff have an educational reason to allow children to use mobile phones or personal devices as part of an educational activity then it will only take place when approved by the Senior Leadership Team.
- Staff should not use personal devices such as mobile phones or cameras to take photos or videos of pupils and will only use work –provided equipment for this purpose.
- If a member of staff breaches the school policy then disciplinary action may be taken.

Community use of the Internet

- The school will liaise with other organizations such as After School Club to establish a common approach to Online Safety.

Communications Policy

Introducing the Online Safety policy to pupils

- The first lesson of every unit within the long term plan of Computing will be focused on online safety using the objectives from 'Education in a connected world'.
- Online safety will be taught through the SCARF PSHE curriculum.
- Online 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.
- A programme of training in onlie safety will run within the school in the form of St Teresa's online safety proficiency certificates.
- Online Safety day is an annual whole school focus with activities for children and parents.
- Online Safety training will be embedded within the Computing curriculum and the Social, Moral, Spiritual and Cultural (SMSC) curriculum.
- Digital Leaders within Y6 will provide information about online safety to all children across the school with the support of the Computing Leader.
- The computing leader will conduct an online safety assembly once a term.
- There will be at least 1 display within a communal area in school informing the children of the importance of online safety.

Staff and the Online Safety policy

- All staff will be given the School Online 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 will always use a child friendly safe search engine when accessing the web with pupils.
- Staff that manage filtering systems or monitor ICT use will be supervised by senior leadership and work to clear procedures for reporting issues.
- Staff should understand that phone or online communications with pupils can occasionally lead to misunderstandings or even malicious accusations. Staff must take care always to maintain a professional relationship.
- Staff will be given regular up-to-date training on Online Safety.

Contextual safeguarding and online safety

- All staff will be made aware of the contextual safeguarding issues linked to online safety, that are likely to arise in the community around St Teresa's Catholic Primary School. An example of this is time spent on online gaming sites due to the fact that many children within the school have access to gaming devises at home.

Enlisting parents' and carers' support

- Parents' and carers' attention will be drawn to the School Online Safety Policy in newsletters, the school brochure and on the school Web site.
- The school will maintain a list of Online Safety resources for parents/carers.
- Teaching and learning consultants from Lancashire will deliver updates and important messages to parents after school.

School website

- The school website will have an area dedicated to informing parents about online safety.
- Links to online safety websites will be listed on the website
- Evidence of online safety work competed within school will be displayed on the website.