St Anne line Catholic Infant School

Online Safety Policy

Dec 2016

This online safety policy is designed to ensure that pupils are protected in an online environment from inappropriate content, contact or conduct.

This policy has been created with reference to the guidance from the Essex Children's Safeguarding Board and Safeguarding Children in Education Policy 2016.

Please see the full policy for Essex Schools which can be found online at www.escb.co.uk for any further information or guidance about our schools procedures.

This policy includes:

- Risks
- Responsibilities
    - governors
    - staff
    - pupils
    - parents

- Teaching and Learning
- Messaging including 'sexting'
- Social Media
- Images and Videos
- Games and Apps
- Emerging technologies/software
- School computer systems
- Reporting Procedures
- Advice for parents

Risks

The Byron review classifies the risks inherent in the use of new technologies as relating to content, contact and conduct and is often determined by behaviours rather than the technologies themselves:

	Commercial	Aggressive	Sexual	Values
Content Child as recipient	Adverts Spam Sponsorship Personal Info	Violent or hateful content	Pornographic Sexual content	Bias Racism Extremism/Terrorism Misleading advice or information
Contact Child as participant	Tracking or harvesting of personal info	Bullying Harassment Stalking	Grooming Meeting Strangers	Self-Harm Unwelcome persuasions
Conduct Child as actor	Illegal downloads Hacking Gambling Financial Scams Extremism/Terrorism	Bullying or harassing another	Creating, uploading, viewing or sending inappropriate material	Providing misleading info or advice

Byron review of Children and new technology (2008) Published by DCSF and DCMS

Content

- Exposure to age-inappropriate material
- Exposure to inaccurate or misleading information
- Exposure to socially unacceptable material, such as that inciting violence, hate or intolerance
- Exposure to illegal material, such as images of child abuse.

Contact

- Grooming using communication technologies to meet and groom children with the intention of sexually abusing them (both on and off line exploitation).

Commerce/Conduct

- Exposure of minors to inappropriate commercial advertising
- Exposure to online gambling services
- Commercial and financial scams

Responsibilities

Governors

- Governors are responsible for reviewing the online safety policy, procedures for reporting and dealing with incidents as part of the schools safeguarding requirements.

Staff

- The head teacher is the designated safeguard leader for the school and incidents are reported to her. She is responsible for monitoring the online safety log.

- The computing/online safety co-ordinator and head teacher are responsible for ensuring staff and parents have up to date information and training for online safety and that policies are updated regularly.
- Teachers are responsible for checking online resources are appropriate and safe for children prior to lessons.
- All staff are responsible for being up to date with online safety and safeguarding training in order to identify and prevent any child protection issues.
- All staff are responsible for ensuring they teach and discuss online safety issues with pupils so they are aware of signs of inappropriate contact, content and conduct and so pupils know what to do and/or who to speak to for help.

Pupils

- Are responsible for knowing how to conduct themselves online in a kind way, as they would face to face.

Parents/Carers

- Parents/carers are to ensure that they monitor their child online checking that they are not exposed to age inappropriate material.
- Parents/carers are responsible for informing the school (head teacher) of any online child protection issues as soon as possible.

Teaching and Learning

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

- The school Internet access will be designed expressly for pupil use including appropriate content filtering.
- Pupils will be given clear objectives for Internet use and taught what use is acceptable and what is not.
- Pupils will be educated in how to use the Internet for research and how to evaluate the truth of information they might find online.
- As part of the Computing curriculum, all year groups will have online safety embedded into their lessons.
- Children will also be taught about online safety through other means such as PSHE sessions and focus days.
- The school will ensure that the use of Internet derived materials by staff and pupils complies with copyright law.
- When children are directed to websites as part of home learning they will have been checked for appropriateness by the teacher setting the learning.

Messaging including ‘sexting’

There are a number of definitions of ‘sexting’ but for the purposes of this policy ‘sexting’ is simply defined as:

- Images or videos generated by children under the age of 18,

- Images or videos of children under the age of 18 that are of a sexual nature or are indecent.

- These images are shared between young people and/or adults via a mobile phone, handheld device, computer, 'tablet' or website with people they may not even know.

We take a pro-active approach to teaching pupils about inappropriate messages including 'sexting' however this is at an age and language appropriate level for the children in our school.

We do this in co-ordination with the NSPCC PANTS campaign and through the use of child friendly, age appropriate books, assemblies and PSHE lessons.

The procedures for cases of 'sexting' should follow normal safeguarding practices and protocols. The incident should be reported to the Head Teacher as the designated safeguarding leader of the school.

The child involved may suffer emotional distress and so the schools Learning Mentor will be available to provide support.

Social Media

Social networking Internet sites (such as Facebook) provide facilities to chat and exchange information online. This online world is very different from the real one with the temptation to say and do things beyond usual face to-face contact.

- Use of social networking sites and newsgroups in the school, is not allowed and will be blocked/filtered.
- Pupils are advised never to give out personal details of any kind that may identify themselves, other pupils, their school or location. This will also include not using personal photographs and videos.

- Pupils and parents are advised that the use of social network spaces outside school is inappropriate for primary aged pupils.

- Parents, pupils and staff will be advised of the dangers of discussing pupils, staff or the school on social networking sites. The governors will consider taking legal action, where appropriate, to protect pupils and staff against cyber bullying and defamatory comments.

Images and Videos

Images and videos are not connected online but can be easily shared and then accessed on the Internet.

- Staff advise pupils about taking, sending and searching for appropriate and/or inappropriate images and videos.

- Pupils are taught what to do if an image or picture makes them feel upset or worried.
- Parents are not to publish any images or videos of other children online.
- We advise parents to consider the safety of their child if they choose publish their image or video online, these pictures may identify their child by their uniform and photographs taken on many modern devices include a geo-locater tag whereby it is very easy to pinpoint where the photo was taken, this is very serious should this information fall into the wrong hands.

Games & Apps

Many children like to keep up the trend by playing digital games online and offline. Online games are like an online playground, however unlike your local park you cannot see who really is in the 'playground'. Many cases of grooming begin by befriending children through games and apps.

- Parents must check the game/app has the appropriate age rating to ensure their child is safeguarded against inappropriate language, images and themes.
- If a child discloses they have played an age inappropriate game/app to staff this must be reported to the head teacher (designated safeguard leader) and recorded in the online safety log, parents will be contacted.
- We advise children that online 'friends' they meet in games or on apps may not be who they say they are. Their new friends kindness may turn unkind. Children are told NEVER to meet anybody they talk to online.

Emerging Technologies/Software

Technology and software changes rapidly with new websites and apps created every day.

- Staff are aware that new websites may not be filtered by the LEA and may occasional be accessible in school. Staff must report any situations such as this immediately to the head teacher (A Russell) or computing co-ordinator (R Bond) who will contact the LEA.
- We will review the risks and benefits of any new apps, games, websites and technology before they are used in the school.

School Computer Systems

The school systems are managed by Essex County Council local authority. They are responsible for filtering and monitoring Internet use in the school.

Reporting Procedures

In order to safeguard and protect our pupils any online safety concerns or issues must be reported immediately to the headteacher as designated safeguard leader.

The online safety incident log is kept in a secure location in the school and demonstrates the protocols and procedures to be taken in the event of an incident.

Parents or staff may report directly to the Child Online Exploitation team who will investigate matters and provide support for families and children.

https://www.ceop.police.uk

Pupils are always encouraged to talk to an adult they trust such as parent or teacher if they feel concerned about something that has happened online. We advise them they will not be punished for doing so.

Advice for parents/carers

It is important to establish and maintain an open approach to online use with your child. This way they understand that they can talk to you about their concerns and it also means they understand that you must check their devices and online activity to ensure they are safe.

Many parents react to issues by taking away their child's device or online access however this results in the child feeling that the next time something happens they won't tell as they don't want their device taken away from them.

With a rapidly changing online world it is important that parents/carers understand exactly what apps and games their child is accessing and the possible risks.

There are many websites with great advice for parents/carers about particular apps, games and approaches to take with their child. Here are some examples:

https://www.nspcc.org.uk/preventing-abuse/keeping-children-safe/

http://www.vodafone.com/content/digital-parenting.html

There are also some good websites where children can access information about how to stay safe online:

https://www.thinkuknow.co.uk/5_7/hectorsworld/

https://www.thinkuknow.co.uk/5_7/leeandkim/

http://www.childnet.com/young-people/primary