English Martyrs Catholic Voluntary Academy
Online Safety Policy

" We learn and grow as a family following in the footsteps of Jesus "

Approved by: FGB **Date:** September 2020

Last reviewed on: September 2020

Next review due by: September 2023

Introduction

English Martyrs Catholic Academy fully recognises the contribution it can make to protect children and support them in school. The aim of this policy is to safeguard and promote our pupils' safe use of internet and electronic communication technology such as mobile phones and wireless connectivity. The internet and other technologies have an important role in the learning and teaching processes however, we feel it is important to balance those benefits with an awareness of the potential risks. This policy will highlight the need to educate children and young people about the benefits and risks of using new technologies both in and away from school.

It will also provide safeguards and rules to guide staff, pupils and visitors in their online experiences. The school online safety policy will operate in conjunction with others including: policies for Safeguarding and child protection, Behaviour, Anti-Bullying, Single Equality and Internet Access Agreement with parents/carers.

The school acknowledges online and security as important issues for our school community and has made a considered attempt to embed online safeguarding into our teaching and learning using technology and have considered the wider implications of online safeguarding beyond classroom practice such as remote learning, security and data.

Effective Practice in On line safety.

Online safety depends on effective practice in each of the following areas:

- Education for responsible ICT use by staff and pupils;
- A comprehensive, agreed and implemented Online safety Policy;
- Secure, filtered broadband
- The use of online safety control software monitoring system which monitors and captures inappropriate words or web sites used.

Our Aims

- **To have robust processes in place to ensure the online safety of children, staff, volunteers and governors.**
- **To deliver an effective approach to online safety which empowers us to protect and educate the whole school community in its use of technology.**
- **To establish clear mechanisms to identify, intervene and escalate an incident where appropriate.**

Legislation and guidance

This policy is based on the Department for Education's (DfE) statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on:

- Teaching online safety in schools
- Preventing and tackling bullying and cyber-bullying: advice for headteachers and school staff
- RSE curriculum.
- Searching, screening and confiscation

It also refers to the Department's guidance on protecting children from radicalisation.

It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils' electronic devices where they believe there is a 'good reason' to do so.

The policy also takes into account the National Curriculum computing programmes of study and curriculum support provided through the Knowsley scheme of work.

United Nations Convention on the Right of the Child

Article 17

You have the right to get information that is important to your well-being, from radio, newspaper, books, computers and other sources. Adults should make sure that the information you are getting is not harmful, and help you find and understand the information you need.

ICT in the 21st Century is seen as an essential resource to support learning and teaching, as well as playing an important role in the everyday lives of children, young people and adults. Consequently, schools need to build in the use of these technologies in order to arm our young people with the skills to access life-long learning and employment.

Information and Communications Technology covers a wide range of resources including; web-based and mobile learning. It is also important to recognise the constant and fast paced evolution of ICT within our society as a whole.

Currently the internet technologies children and young people are using both inside and outside of the classroom include:

- Websites
- Virtual Learning Platforms
- Email and Instant Messaging
- Chat Rooms and Social Networking

- Forums, Wikis and Blogs
- Podcasting
- Video Broadcasting
- Music Downloading
- Gaming
- Mobile devices with web functionality

Whilst exciting and beneficial both in and out of the context of education, much ICT, particularly web-based resources, are not consistently policed. All users need to be aware of the range of risks associated with the use of these Internet technologies. We understand the responsibility to educate our pupils on safety issues; teaching them the appropriate behaviours and critical thinking skills to enable them to remain both safe and legal when using the internet and related technologies, in and beyond the context of the classroom.

Some of the potential dangers of using technology may include:

- Access to illegal, harmful or inappropriate images or other content
- Unauthorised access to/loss of/sharing of personal information
- The risk of being subject to grooming by those with whom they make contact on the internet.
- The sharing/distribution of personal images without an individual's consent or knowledge
- Inappropriate communication/contact with others, including strangers
- Cyber-bullying
- Access to unsuitable video/internet games
- An inability to evaluate the quality, accuracy and relevance of information on
- the internet
- Plagiarism and copyright infringement
- Illegal downloading of music or video files
- The potential for excessive use which may impact on the social and emotional development and learning of the young person.

Many of these risks reflect situations in the offline world but it is important that as a school we have a planned and coordinated approach to ensuring that all involved with the school use technology in a safe and responsible way. As with all risks it is impossible to eliminate them completely but with a planned and coordinated approach they can be significantly reduced and users can be taught to manage them effectively.

Both this policy and the Acceptable Use Agreement (for all staff, governors, visitors and pupils) are inclusive of both fixed and mobile internet; technologies provided by the school (such as PCs, laptops, tablets, webcams, whiteboards, digital video equipment, cameras etc); and technologies owned by pupils and staff, but brought onto school premises utilising the school's network (such as laptops, mobile phones, camera phones, PDAs and portable media players, etc).

End to End Online Safety

E-Safety depends on effective practice at a number of levels:

• Responsible ICT use by all staff and students; encouraged by education and made explicit through published policies.

- Sound implementation of e-safety policy in both administration and curriculum, including secure school network design and use.

- Safe and secure broadband Network including the effective management of LEA preferred filtering product.

- Use of National Education Network E-Safety standards and specifications based on their current research and findings.

Access at: http://www.nen.gov.uk/files/NEN_Internet_Safety_Research_Final_Report.pdf

Roles and Responsibilities

The governing board

The governing board has overall responsibility for monitoring this policy and holding the head teacher to account for its implementation.

The governing board will co-ordinate regular meetings with appropriate staff to discuss online safety, and monitor online safety logs as provided by the designated safeguarding lead (DSL).

The governor who oversees safeguarding and online safety is D Bonnano.

All governors will:

- Ensure that they have read and understand this policy
- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet

The headteacher

The head teacher is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.

The designated safeguarding lead

Details of the school's DSL and deputy/deputies are set out in our child protection and safeguarding policy.

The DSL takes lead responsibility for online safety in school, in particular:

- Supporting the head teacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the head teacher and other staff, as necessary, to address any online safety issues or incidents
- Ensuring that any online safety incidents are logged and dealt with appropriately in lin e with this policy
- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy
- Updating and delivering staff training on online safety
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in school to the head teacher and/or governing board

This list is not intended to be exhaustive.

This policy, supported by the school's acceptable use agreements for staff, governors, visitors and pupils (appendices), is to protect the interests and safety of the whole school community. It is linked to the following mandatory school policies: **Safeguarding, Health and Safety, Home–School agreements, and behaviour (including the anti-bullying) policy.**

The ICT manager – The Ark

The ICT manager is responsible for:

- Putting in place appropriate filtering and monitoring systems, which are updated on a regular basis and keep pupils safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material
- Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Conducting a full security check and monitoring the school's ICT systems on a regular basis
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files

This list is not intended to be exhaustive.

All staff and volunteers

All staff, including contractors and agency staff, and volunteers are responsible for:

- Maintaining an understanding of this policy
- Implementing this policy consistently
- Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet and ensuring that pupils follow the school's terms on acceptable use.
- Working with the DSL to ensure that any online safety incidents are logged and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy

This list is not intended to be exhaustive.

Parents

Parents are expected to:

- Notify a member of staff or the head teacher of any concerns or queries regarding this policy
- Ensure their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet in the home, school policy.

Parents can seek further guidance on keeping children safe online from the following organisations and websites:

- What are the issues? - UK Safer Internet Centre
- Hot topics - Childnet International
- Parent factsheet - Childnet International

Visitors and members of the community

Visitors and members of the community who use the school's ICT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it.

Educating children about online safety.

Pupils will be taught about online safety as part of the curriculum through the Knowlesey scheme of work which supports the National curriculum computing programmes of study:

The text below is taken from the National Curriculum computing programmes of study.

In **Key Stage 1**, pupils will be taught to:

- Use technology safely and respectfully, keeping personal information private
- Identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies

Pupils in **Key Stage 2** will be taught to:

- Use technology safely, respectfully and responsibly
- Recognise acceptable and unacceptable behaviour
- Identify a range of ways to report concerns about content and contact

RSE curriculum - By the ***end of primary school****, pupils will know:*

- *That people sometimes behave differently online, including by pretending to be someone they are not.*
- *That the same principles apply to online relationships as to face-to-face relationships, including the importance of respect for others online including when we are anonymous*
- *The rules and principles for keeping safe online, how to recognise risks, harmful content and contact, and how to report them*
- *How to critically consider their online friendships and sources of information including awareness of the risks associated with people they have never met*
- *How information and data is shared and used online*
- *How to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know*

The safe use of social media and the internet will also be covered in other subjects where relevant.

The school will use assemblies to raise pupils' awareness of the dangers that can be encountered online and may also invite speakers to talk to pupils about this.

Online Safety skills development for staff

- Our staff receive regular information and annual training on Online Safety issues in the form of regular staff training.
- Details of the ongoing staff training programme can be found in the CPD record.
- New staff receive information on the online safety policy as part of their induction process.
- All staff have been made aware of individual responsibilities relating to the safeguarding of children within the context of online safety and know what to do in the event of misuse of technology by any member of the school community.
- All staff incorporate online safety activities and awareness within the computing curriculum, PSHE teaching and other curriculum areas where appropriate.

Educating parents about online safety

- The school will raise parents' awareness of internet safety in letters or other communications home, and in information via our website or class dojo / tapestry. This policy will also be shared with parents.
- Online safety will also be covered during parents' evenings.

- If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the head teacher and/or the DSL.
- Parents/ carers are asked to read through and sign acceptable use agreements on behalf of their child on admission to school.
- The school disseminates information to parents relating to eSafety where appropriate in the form of;
  - ✓ Information and celebration evenings / assesmblies
  - ✓ Posters
  - ✓ Website
  - ✓ Newsletter items

Password Security

- All users read and sign an Acceptable Use Agreement to demonstrate that they have understood the school's online safety Policy.
- Users are provided with an individual network, email and log-in username.
- Pupils are not allowed to deliberately access on-line materials or files on the school network, of their peers, teachers or others.
- If you think your password may have been compromised or someone else has become aware of your password report this to the Head teacher
- Staff are aware of their individual responsibilities to protect the security and confidentiality of school networks, including ensuring that passwords are not shared and are changed periodically. Individual staff users must also make sure that workstations are not left unattended and are locked.

Data Security

The accessing of school data is something that the school takes very seriously. Staff are aware of their responsibility when accessing school data. They must not;

- allow others to view the data
- edit the data unless specifically requested to do so by the Head teacher.
- If staff are taking data off site it must be password protected.

Please refer to the trust GDPR policy.

Managing the Internet

The internet is an open communication medium, available to all, at all times. Anyone can view information, send messages, discuss ideas and publish material which makes it both an invaluable resource for education, business and social interaction, as well as a potential risk to young and vulnerable people. All use of English Martyrs Internet Web Filtering Systems is logged and the logs are randomly monitored. Whenever any inappropriate use is detected it will be followed up by Lincolnshire Safeguarding Children Board (LSCB) E Safety Officer through its eSafety responsibilities.

- Pupils will have supervised access to Internet resources (where reasonable) through the school's mobile internet technology.
- Staff will preview any recommended sites before use.
- Raw image searches are discouraged when working with pupils.

- If Internet research is set for homework, specific sites will be suggested that have previously been checked by the teacher. It is advised that parents recheck these sites and supervise this work.
- Parents will be advised to supervise any further research.
- All users must observe software copyright at all times. It is illegal to copy or distribute school software or illegal software from other sources.
- All users must observe copyright of materials from electronic resources.

Cyber-bullying

Definition

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of one person or group by another person or group, where the relationship involves an imbalance of power. (See also the school behaviour and anti bullying policy.)

Preventing and addressing cyber-bullying

To help prevent cyber-bullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

The school will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Class teachers will discuss cyber-bullying with their tutor groups, and the issue will be addressed in assemblies.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes personal, social, health and economic (PSHE) education, and other subjects where appropriate.

All staff, governors and volunteers receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training.

The school also sends information/leaflets on cyber-bullying to parents so that they are aware of the signs, how to report it and how they can support children who may be affected.

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school behaviour policy. Where illegal, inappropriate or harmful material has been spread among pupils, the school will use all reasonable endeavours to ensure the incident is contained.

The DSL will consider whether the incident should be reported to the police if it involves illegal material, and will work with external services if it is deemed necessary to do so.

Examining electronic devices

School staff have the specific power under the Education and Inspections Act 2006 (which has been increased by the Education Act 2011) to search for and, if necessary, delete inappropriate images or files on pupils' electronic devices, including mobile phones, iPads and other tablet devices, where they believe there is a 'good reason' to do so.

When deciding whether there is a good reason to examine or erase data or files on an electronic device, staff must reasonably suspect that the data or file in question has been, or could be, used to:

- Cause harm, and/or
- Disrupt teaching, and/or
- Break any of the school rules

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL or other member of the senior leadership team to decide whether they should:

- Delete that material, or
- Retain it as evidence (of a criminal offence or a breach of school discipline), and/or
- Report it to the police

Any searching of pupils will be carried out in line with the DfE's latest guidance on screening, searching and confiscation.

Any complaints about searching for or deleting inappropriate images or files on pupi ls' electronic devices will be dealt with through the school complaints procedure.

Email

The use of email within most schools is an essential means of communication for both staff and pupils. In the context of school, email should not be considered private. Educationally, email can offer significant benefits including; direct written contact between schools on different projects, be they staff based or pupil based, within school or international. We recognise that pupils need to understand how to style an email in relation to their age and good 'netiquette'.

- The school gives all staff their own email account to use for all school business. This is to minimise the risk of receiving unsolicited or malicious emails and avoids the risk of personal profile information being revealed.
- It is the responsibility of each account holder to keep the password secure. For the safety and security of users and recipients, all mail is filtered and logged; if necessary email histories can be traced. This should be the account that is used for all school business.
- Under no circumstances should staff contact pupils, parents or conduct any school business using personal email addresses.
- All e-mail users are expected to adhere to the generally accepted rules of network etiquette (netiquette) particularly in relation to the use of appropriate language and not revealing any personal details about themselves or others in e-mail communication, or arrange to meet anyone without specific permission, virus checking attachments.
- Pupils are introduced to email as part of the IT Scheme of Work.
- Pupils may only use approved e-mail accounts on the school system.
- Pupils must immediately tell a teacher if they receive offensive e-mail.
- Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.
- Staff must inform Head teacher if they receive an offensive e- mail.
- The forwarding of chain letters this includes jokes and funny statements is not permitted in school.

Published content and the school web site

The contact details on the website should be the school address, e-mail and telephone number. Staff or pupils' personal information will not be published.

The Head teacher will take overall editorial responsibility and ensure that content is accurate and appropriate. The advice for using photographs on a website is no different from their use in any other kind of publication or publicity material. However, the staff and governors of English Martyrs are aware of the potential risk of inappropriate use of images because of the lack of control over who might see the image and the wide extent of the misuse of the Internet by certain people. The school will seek the consent of parents regarding the use of images on the Internet. Children's surnames will not be included in photographs of children published on the school website.

The Press

The use of photographs in newspapers and magazines is already subject to strict guidelines.
The Press Complaints Commission's Code of Practice states that:

- Journalists must not interview or photograph a child under the age of 16 on subjects involving the welfare of the child in the absence of or without the consent of a parent or other adult who is responsible for the children.

- Pupils must not be approached or photographed while at school without the permission of the school authorities.
- There is no breach of the Data Protection Act 1998 in passing on a child's name to a journalist as long as parental consent has been secured.

Filming Events

It is usual for parents to take photographs and videos of children at school events such as the annual Nativity Play and Sports Day. Any objections to this policy should be addressed to the Head teacher. The school will seek the consent of parents / guardians regarding the use of photographs/film of children at these events and take into account the wishes of all parents / guardians. On occasions, commercial video films may be made of children on educational visits and performing in school productions. The school will inform parents where arrangements have been made for a commercial photographer to film such an event.

Where a commercial photographer is used, the school will follow the NSPCC guidelines which are as follows: Schools should provide a clear brief about what is considered appropriate in terms of content and behaviour; Schools should issue the photographer with identification which must be worn at all times; Schools should let parents and children know that a photographer will be in attendance at an event and ensure they consent to both the taking and publication of films and photographs; Schools should not allow unsupervised access to children or one-to-one photo sessions at home; Schools should not approve / allow photo sessions outside the event or at a child's home.

Mobile Technologies

Many emerging technologies offer new opportunities for teaching and learning including a move towards personalised learning and 1:1 device ownership for children and young people. Many existing mobile technologies such as portable media players, Tablets, gaming devices, mobile and Smart phones are familiar to children outside of school too. They often provide a collaborative, well- known device with possible internet access and thus open up risk and misuse associated with communication and internet use. Emerging technologies will be examined for educational benefit and the risk assessed before use in school is allowed. Our school chooses to manage the use of these devices in the following ways so that users exploit them appropriately.

Personal Mobile Devices (including phones)

- The school allows staff to bring in personal mobile phones and devices for their own use. Under no circumstances does the school allow a member of staff to contact a pupil or parent/ carer using their personal device. Personal mobile phones must be kept in the staff room or secured safely, they must not be on show in the classroom. All visitors and governors will be asked to place their mobile phones in a secure place.
- Pupils are not allowed to bring personal mobile devices/phones to school unless with the prior approval of the school. If phones are needed for after school if walking home alone, they must be handed into the office before school and picked up at the end of the day. A permission letter from the parent must be signed.
- The school is not responsible for the loss, damage or theft of any personal mobile device.
- The sending of inappropriate text messages or emails between any member of the school community is not allowed.
- Permission must be sought before any image or sound recordings are made on these devices of any member of the school community.
- Users bringing personal devices into school must ensure there is no inappropriate or illegal content on the device.
- Staff should not contact pupils outside normal school hours.
- The sending of inappropriate text messages between any member of the school community is not allowed.
- Permission must be sought before any image or sound recordings are made on the devices of any member of the school community.
- Where the school provides mobile technologies such as laptops and Tablets for offsite visits and trips, only these devices should be used.
- Where the school provides a laptop for staff, only this device may only be used to conduct school business outside of school.

The Safe Use of Children’s Photographs

Schools need and welcome publicity. Children’s photographs add colour, life and interest to articles promoting school activities and initiatives. Making use of photographs for publicity materials and to promote the school in the press can increase pupil motivation and staff morale, and help parents and the local community identify and celebrate the school's achievements. However, photographs must be used in a responsible way. Schools need to respect children's and parents' rights of privacy and be aware of potential child protection issues.

Every reasonable effort will be made to minimise risk by following the guidelines detailed in this document and by securing parental consent for the use of photographs.

English Martyrs will not display images of pupils or staff on websites, in publications or in a public place without such consent. The definition of a public place includes areas where visitors to the school have access. Where photographs are taken at an event attended by large crowds, this is regarded as a public area so it is not necessary to get permission of everyone in a crowd shot. The Data Protection Act does not apply to photographs or films taken for personal use by family and friends.

The development of digital imaging technologies has created significant benefits to learning, allowing school staff and pupils instant use of images they have recorded themselves or downloaded from the internet. School staff and pupils are made aware of the potential risks associated with storing, sharing and posting images on the internet and must follow the good practice detailed below.

Digital images are easy to capture, reproduce and publish and, therefore, misused. We must remember that it is not always appropriate to take or store images of any member of the school community or public, without first seeking consent and considering the appropriateness.

- With the written consent of parents (on behalf of pupils) and staff, the school permits the appropriate taking of images by staff and pupils with school equipment.
- Staff are not permitted to use personal digital equipment, such as mobile phones and cameras, to record images of pupils, this includes when on field trips. However, with the express permission of the Head teacher, images can be taken provided they are transferred immediately and solely to the school's network and deleted from the staff device.

<u>Publishing pupil's images and work</u>

On a child's entry to the school, all parents/guardians will be asked to give permission to use their child's work/photos in the following ways:

- on the school web site and information screen in front entrance.
- in the school prospectus and other printed publications that the school may produce for promotional purposes recorded/ transmitted on a video or webcam
- in display material that may be used in the school's communal areas
- in display material that may be used in external areas, ie exhibition, promoting the school

- general media appearances, e.g. local/ national media/ press releases sent to the press highlighting an activity (sent using traditional methods or electronically)
- This consent form is considered valid for the entire period that the child attends this school unless there is a change in the child's circumstances where consent could be an issue, e.g. divorce of parents, custody issues, etc. Parents/ carers may withdraw permission, in writing, at any time. Consent has to be given by both parents in order for it to be deemed valid. Pupils' surnames names will not be published alongside their image and vice versa. E-mail and postal addresses of pupils will not be published.

Storage of Images

- Images/ films of children are stored on the school's network
- Pupils and staff are not permitted to use personal portable media for storage of images (e.g., USB sticks) without the express permission of the Head teacher
- Rights of access to this material are restricted to the teaching and support staff and pupils within the confines of the school network

Social Networking and Personal Publishing

- The school will block/filter access to social networking sites.
- Newsgroups will be blocked unless a specific use is approved.
- Pupils will be told never to give out personal details of any kind which may identify them or their location.

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 by the IT governor, the DSL and Head Teacher.

Assessing Risks

- The school will take all reasonable precautions to ensure that users access only appropriate 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 school computer. Neither the school nor trust can accept liability for the material accessed, or any consequences of Internet access.
- The school will audit ICT provision to establish if the online safety policy is adequate and that its implementation is effective.

Complaints

Complaints relating to online safety should be made to the DSL or Head teacher. Incidents should be logged. Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.

Pupils and parents will be informed of the complaints procedure. Advice would be sought from the trust in the event the school needed to establish procedures for handling potentially illegal issues.

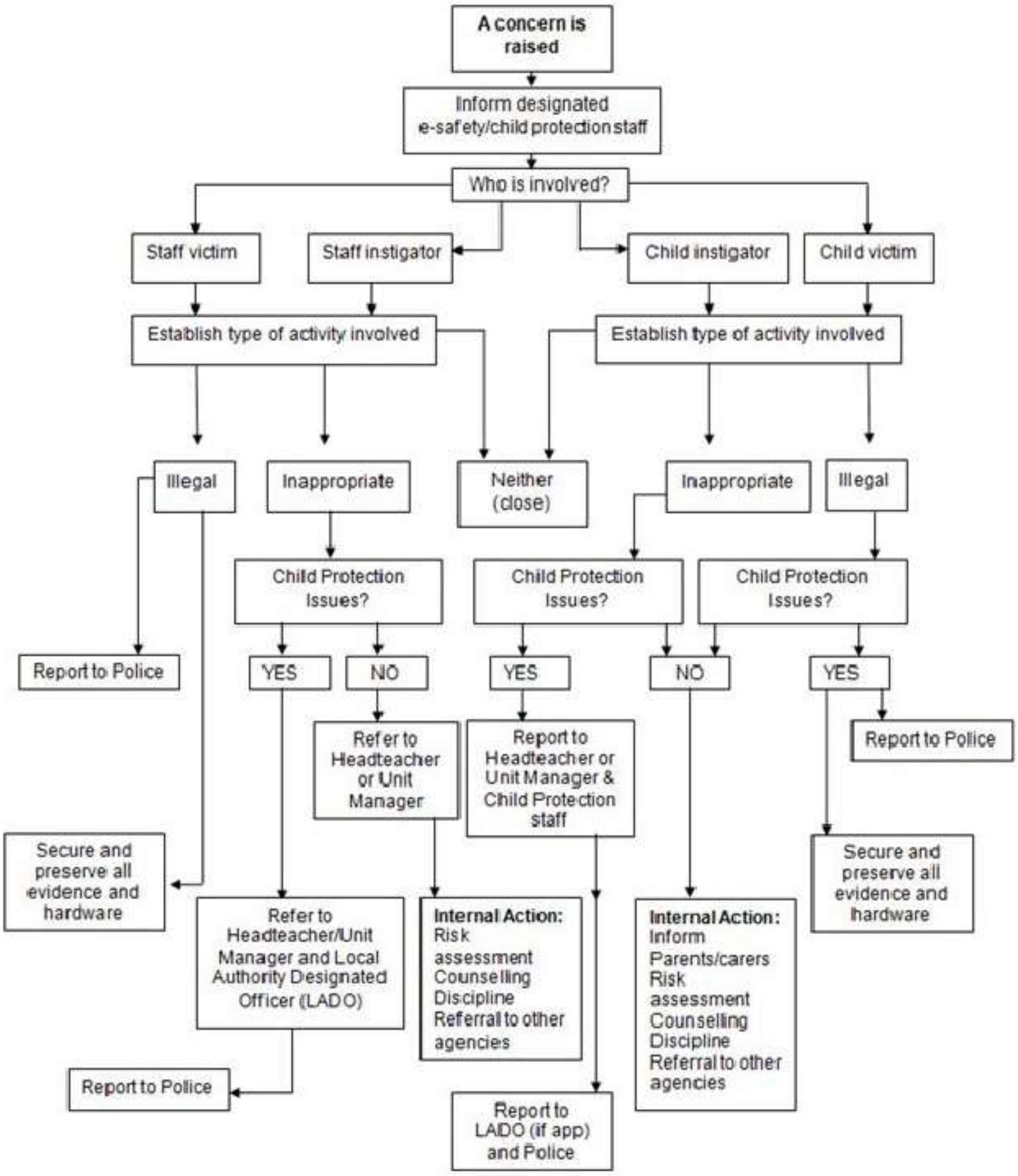
Equal Opportunities - Pupils with additional needs

The school endeavours to create a consistent message with parents for all pupils and this in turn should aid establishment and future development of the schools online safety rules. However, staffs are aware that some pupils may require additional teaching including reminders, prompts and further explanation to reinforce their existing knowledge and understanding of online safety issues.

Where a pupil has poor social understanding, careful consideration is given to group interactions when raising awareness of online safety. Internet activities are planned and well managed for these children.

Responding to incidents of misuse

It is hoped that all members of the school community will be responsible users of IT, who understand and follow this policy. However, there may be times when infringements of the policy could take place accidently, through careless or irresponsible or, very rarely, through deliberate misuse. In the event of an safety incident it is important that there is a considered, coordinated and consistent approach. Incidents will be managed using the incident flowchart below.


A concern is raised
Inform designated e-safety/child protection staff
Who is involved?
Staff victim
Staff instigator
Child instigator
Child victim
Establish type of activity involved
Establish type of activity involved
Illegal
Inappropriate
Neither (close)
Inappropriate
Illegal
Child Protection Issues?
Child Protection Issues?
Child Protection Issues?
Report to Police
YES
NO
YES
NO
YES
Report to Police
Refer to Headteacher or Unit Manager
Report to Headteacher or Unit Manager & Child Protection staff
Secure and preserve all evidence and hardware
Secure and preserve all evidence and hardware
Refer to Headteacher/Unit Manager and Local Authority Designated Officer (LADO)
Internal Action: Risk assessment Counselling Discipline Referral to other agencies
Internal Action: Inform Parents/carers Risk assessment Counselling Discipline Referral to other agencies
Report to Police
Report to LADO (if app) and Police

Appendix 1

English Martyrs Catholic Voluntary Academy

Acceptable Use Agreement / Code of Conduct

IT and the related technologies such as email, the internet and mobile devices are an expected part of our daily working life in school. This policy is designed to ensure that all staff are aware of their professional responsibilities when using any form of IT. All staff are expected to sign this policy and adhere at all times to its contents.
Any concerns or clarification should be discussed with the Head teacher.

- I will only use the school's email / Internet and any related technologies for professional purposes or for uses deemed 'reasonable' by the Head or Governing Body.
- I will comply with the IT system security and not disclose any passwords provided to me by the school or other related authorities.
- I will ensure that all electronic communications with pupils and staff are compatible with my professional role.
- I will not give out my own personal details, such as mobile phone number and personal email address, to pupils.
- I will ensure my personal mobile phone is not visible in the classroom or used for school business.
- I will only use the approved, secure email system(s) for any school business.
- I will ensure that personal data is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely. Personal data can only be taken out of school or accessed remotely when authorised by the Head.
- I will not browse, download, upload or distribute any material that could b considered offensive, illegal or discriminatory.
- Images of pupils and/ or staff will only be taken, stored and used for professional purposes in line with school policy and with written consent of the parent, carer or staff member. Images will not be distributed outside the school network without the permission of the parent/ carer, member of staff or Headteacher.
- I understand that all my use of the Internet and other related technologies can b monitored and logged and can be made available, on request, to the Headteacher.
- I will respect copyright and intellectual property rights.
- I will ensure that my online activity, both in school and outside school, will not bring my professional role into disrepute.
- I will support and promote the school's Online Safety policy and help pupils to be safe and responsible in their use of IT and related technologies.

User Signature

I agree to follow this code of conduct and to support the safe use of IT throughout the school

Signature ………………………………… Date ……………………

Job title …………………………………………………………………………….

Full Name ………………………………………………………………………(print)

Appendix 2 Technology Matrix

Communication technologies	Staff and other adults				Pupils			
	Allowed	Allowed at certain times	Allowed for selected	Not allowed	Allowed	Allowed at certain times	Allowed with Head teacher permission	Not allowed
Mobile phones may be brought to school	X						X	
Use of mobile phones in lessons				X				X
Use of mobile phones in social time		X						X
Taking photos on mobile phones				X				X
Taking photos on other camera devices			X				X	
Use of hand held devices e.g. PSPs			X			X		
Use of personal email addresses in school, or on school network			x					X
Use of school emails for personal emails			X					X
Use of chat rooms/ facilities				X				X
Use of instant messaging				X				X
Use of social networking sites				X				X
Use of blogs			X			X		