English Martyrs

Catholic Primary School

e-Safety Policy

Mission Statement

Through Christ we believe, inspire, achieve

Background/Rationale

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school.

The internet and other digital and information technologies are powerful tools, which open up new opportunities for everyone. Electronic communication helps teachers and students/pupils learn from each other. These technologies can stimulate discussion, promote creativity and increase awareness of context to promote effective learning. Children and young people should have an entitlement to safe internet access at all times.

The requirement to ensure that children and young people are able to use the internet and related communications technologies appropriately and safely is addressed as part of the wider duty of care to which all who work in schools are bound. The school e-Safety policy should help to ensure safe and appropriate use. The development and implementation of such a strategy should involve all the stakeholders in a child's education from the head teacher and governors to the senior leaders and classroom teachers, support staff, parents, members of the community and the students/pupils themselves.

The use of these exciting and innovative tools in school and at home has been shown to raise educational standards and promote student/pupil achievement. However, the use of these new technologies can put young people at risk within and outside the school. Some of the dangers they may face 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;
- Cyberbullying;
- 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 off-line world and it is essential that this e-Safety policy is used in conjunction with other school policies including the Child Protection, Data Protection and Whole School Behaviour Policies.

As with all other risks, it is impossible to eliminate those risks completely. It is therefore essential, through good educational provision to build students'/pupils' resilience to the risks to which they may be exposed, so that they have the confidence and skills to face and deal with these risks.

The school must demonstrate that it has provided the necessary safeguards to help ensure that they have done everything that could reasonably be expected of them to manage and reduce these risks. The e-Safety policy that follows explains how we intend to do this, while also addressing wider educational issues in order to help young people (and their parents/carers) to be responsible users and stay safe while using the internet and other

communications technologies for educational, personal and recreational use.

Associated School Policies

This Policy should be read in conjunction with the following school policies/procedures:

- Child Protection & Safeguarding Policy
- Data Protection Policy
- Health and Safety Policy
- Procedures for Using Pupils Images
- Behaviour Policy
- Anti-Bullying Policy

The school will monitor the impact of the policy using:

- *Logs of reported incidents in green file*
- *Pupil and staff interviews.*
- *Annual consultations and reports to parents with reply slips.*

Scope of the Policy

This policy applies to all members of the school community (including staff, students/pupils, governors, volunteers, parents/carers, visitors, community users) who have access to and are users of school ICT systems, both in and out of school.

The Education and Inspections Act 2006 empowers Head teachers, to such extent as is reasonable, to regulate the behaviour of students/pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyberbullying, or other e-Safety related incidents covered by this policy, which may take place out of school, but is linked to membership of the school.

The school will deal with such incidents within this policy and the Whole School Behaviour Policy which includes anti-bullying and will, where known, inform parents/carers of incidents of inappropriate e-Safety behaviour that take place out of school.

Roles and Responsibilities

The following section outlines the roles and responsibilities for e-Safety of individuals and groups within the school:

Governors

Governors are responsible for the approval of the e-Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the chair of governors in their role as e-safety coordinator. He will be supported by the e-safety working party including a parent governor and headteacher. The governing body sub-group for Safeguarding will take responsibility for ensuring the policy is reviewed. An annual report will be provided by the e-safety governor on the implementation and monitoring of the policy at the AGM.

The role of the e-Safety Governor / coordinator will include:
Regular monitoring of e-Safety incident logs
Reporting to relevant Governors committee/meeting

Head teacher and Senior Leaders

The Head teacher is responsible for ensuring the safety (including e-Safety) of members of the school community, though the day to day responsibility for e-Safety will be delegated to the e-Safety Co-ordinator. However, all staff would be expected to have a shared responsibility.
The Head teacher is responsible for ensuring that the e-Safety Coordinator and relevant staff receive suitable CPD to enable them to carry out their e-Safety roles and to train other colleagues, as relevant.
The Headteacher and Governors will receive regular monitoring reports from the e-Safety Coordinator.
The Head teacher and the Assistant Head should be aware of the procedures to be followed in the event of a serious e-Safety allegation being made against a member of staff (see flow chart on dealing with e-Safety incidents – Appendix F, and relevant Local Authority HR/school disciplinary procedures). The procedures for dealing with allegations against staff can be found within the school Child Protection Policy.

e-Safety Coordinator

leads the e-Safety Committee;
takes day to day responsibility for e-Safety issues and has a leading role in establishing and reviewing the school e-Safety policies/documents;
ensures that all staff are aware of the procedures that need to be followed in the event of an e-Safety incident taking place;
facilitates training and advice for staff;
liaises with the Local Authority (where appropriate);
liaises with school's ICT technical support staff;
receives reports of e-Safety incidents and creates a log (green file) of incidents to inform future e-Safety developments;
meets regularly with e-Safety working party to discuss current issues, review incident logs and any other relevant issues.
attends relevant meeting/committee of Governors;
reports regularly to School Staff.

Network Manager/Technical staff

The Network Manager/Systems Manager/ICT Technician/ICT Co-ordinator is responsible for ensuring:
that the school's ICT infrastructure is secure and is not open to misuse or malicious attack;
that the school meets the e-Safety technical requirements outlined in the School e-safety / Acceptable Use Policy and any relevant Local Authority e-Safety Policy and guidance;
that users may only access the school's networks through a properly enforced password protection policy, in which staff are encouraged to change their passwords regularly;
the school's filter is provided by the broadband provider and is regularly monitored for effectiveness.
that he/she keeps up to date with e-Safety technical information in order to effectively carry out their e-Safety role and to inform and update others as relevant;
that the use of the *network/website /remote access/email* is regularly monitored in order that any misuse/attempted misuse can be reported to the *Head teacher for investigation/action/sanction.*

Teaching and Support Staff

Are responsible for ensuring that:
they have an up to date awareness of e-Safety matters and of the current school e-Safety policy and practices;
they have read, understood and signed the Staff Acceptable Use Policy/Agreement (AUP) – see Appendix B.
they report any suspected misuse or problem to the e-Safety Co-ordinator and or Head teacher for investigation.
digital communications with pupils should be on a professional level and only carried out using official school systems.
e-Safety is embedded in all aspects of the curriculum and other school activities.
pupils understand and follow the school e-Safety and acceptable use policy/Agreement – see Appendix A;

they monitor ICT activity in lessons, extra-curricular and extended school activities;
they are aware of e-Safety issues related to the use of mobile phones, cameras and hand held devices.
in lessons where internet use is pre-planned pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.

Designated Safeguarding Lead (DSL)

should be trained in e-Safety issues and be aware of the potential for serious child protection issues to arise from:

- sharing of personal data;
- access to illegal/inappropriate materials;
- inappropriate on-line contact with adults/strangers;
- potential or actual incidents of grooming;
- cyberbullying.

e-Safety Working Party

Members of the e-Safety working party will assist the e-Safety Coordinator with:
The production/review/monitoring of the school e-Safety policy/documents.

Pupils

Taking into account the age and level of understanding of our young pupils:
Will be guided in using the school ICT systems in accordance with the Pupil Acceptable Use Policy/Agreement and Think then Click guidelines – see Appendix A & C, which their parents/carers will be expected to sign before being given access to the internet;
Need to understand the importance of reporting inappropriate content. Should know the importance of adopting good e-safety practices at home.

Parents/Carers

Parents/Carers play a crucial role in ensuring that their children understand the need to use the internet/mobile devices in an appropriate way. Research shows that many parents and carers do not fully understand the issues and are less experienced in the use of ICT than their children. The school will therefore take every opportunity to help parents understand these issues through information guidance on e-safety. Parents and carers will be responsible for:
Endorsing (by signature) the Pupil Acceptable Use Policy/Agreement (AUPA) – see Appendix B;
Ensuring that their children(s) peer on peer interactions online are age-appropriate and suitable;
Ensuring that they themselves do not use the internet/social network sites/other forms of technical communication in an inappropriate or defamatory way.

Community Users

Community Users who access school ICT systems/website as part of the Extended School provision will be expected to sign a AUP before being provided with access to school systems – see Appendix D.

Teaching and Learning

Why Internet use is Important

Internet use is part of the statutory curriculum and is a necessary tool for learning.
The Internet is a part of everyday life for education.
The school has a duty to provide pupils with safe Internet access as part of their learning experience.
Pupils use the Internet widely outside school and need to learn how to question information from the internet and to take care of their own safety and security.
The purpose of Internet use in school is to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the school's management functions.

How Internet Use Benefits Education

Benefits of using the Internet in education include:
access to worldwide educational resources including museums and art galleries;
inclusion in the National Education Network (NEN) which connects all UK schools
educational and cultural exchanges between pupils worldwide;
vocational, social and leisure use in libraries, clubs and at home;
access to experts in many fields for pupils and staff;
professional development for staff through access to national developments, educational materials and effective curriculum practice;
collaboration across networks of schools, support services and professional associations;
improved access to technical support including remote management of networks and automatic system updates;
exchange of curriculum and administration data with the Local Authority and DfE;
access to learning wherever and whenever convenient.

How Internet Use Enhances Learning

The school's Internet access will be used to enhance and extend pupils' independent learning.
Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.
Staff should guide pupils to online activities that will support the learning outcomes planned for the pupils' age and ability.
Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.

How Pupils will Learn How to Evaluate Internet Content

Pupils will be taught to be critically aware of the materials they read and shown how to check the accuracy of information. (advise use several sources of information)
Pupils will use age-appropriate tools to research Internet content.

Pupils with Additional Needs

At English Martyrs Catholic Primary School we strive to meet the needs of every child and take into account that some of our pupils may require extra support or a personalised plan to ensure they are given appropriate access to e-safety information.
A fundamental part of teaching e-Safety is to check pupil's understanding and knowledge of general personal safety issues. Some pupils may need additional teaching that includes reminders and explicit prompts to link their existing knowledge of "how to keep safe" to the rules that will apply specifically to, for instance, internet use.
It might be helpful to consider presenting the rules as being linked to consequences such that you are teaching cause-effect rather than a list of procedures. This needs to be achieved carefully so as to use realistic and practical examples of what might happen if… **without frightening pupils**.

Managing Information Systems

Maintaining Information Systems Security

The security of the school information systems and users will be reviewed regularly.
Virus protection will be updated regularly.
Personal data sent over the Internet or taken off site will be encrypted (Flowcrypt).
Portable media may not be used without specific permission followed by an anti-virus/malware scan.
Unapproved software will not be allowed in work areas or attached to email.
Files held on the school's network will be regularly checked.
The ICT coordinator/network manager will review system capacity regularly.
Use of user logins and passwords to access the school network will be enforced – see below.

The school broadband suppliers are Virgin Media and technical support is provided by Pentre Tech (Steve Sinnott).

Password Security

The school will be responsible for ensuring that the school infrastructure/network is as safe and secure as is reasonably possible and that:
users can only access data to which they have right of access;
no user should be able to access another's files, without permission (or as allowed for monitoring purposes within the school's policies);
access to personal data is securely controlled in line with the school's personal data policy;
logs are maintained of access by users and of their actions while users of the system.
A safe and secure username/password system is essential if the above is to be established and will apply to all school ICT systems including email).
The management of password security will be the responsibility of (network manager)

Responsibilities:
All staff will have responsibility for the security of their username and password, must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security.
Any changes carried out must be notified to the member of staff responsible for issuing and co-ordinating password security.
Users will change their passwords every 6 months.

Training/Awareness:
It is essential that users are made aware of the need to keep passwords secure, and the risks attached to unauthorised access/data loss.

Members of staff will be made aware of the school's password security procedures:
at induction;
through the school's e-Safety policy;
through the Acceptable Use Agreement;
Students will be made aware of the school's password security procedures.

Policy Statements:
All users will have clearly defined access rights to school ICT systems. Details of the access rights available to groups of users will be recorded by the Network Manager.

Audit/Monitoring/Reporting/Review:
The network manager will ensure that full records are kept of:
User IDs and requests for password changes;
User log-ons;
Security incidents related to this policy.

In the event of a serious security incident, the police may request and will be allowed access to passwords used for encryption. Local Authority Auditors also have the right of access to passwords for audit investigation purposes. User lists, IDs and other security related information must be given the highest security classification and stored in a secure manner (safe).

Managing Email

Currently pupils do not use individual email accounts. However, should school or government policy change the following guidelines will be followed: Pupils may only use approved email accounts for school purposes.

Pupils must immediately tell a designated member of staff if they receive offensive email.
Pupils must not reveal personal details of themselves or others in email communication, or arrange to meet anyone without specific permission from an adult.
Whole-class or group email addresses will be used in primary schools for communication outside of the school.
Staff will only use official school provided email accounts to communicate with pupils and parents/carers, as approved by the Headteacher.
Access in school to external personal email accounts may be blocked.
Excessive social email use can interfere with learning and will be restricted.
Email sent to external organisations should be written carefully and authorised before sending, in the same way as a letter written on school headed paper would be.
The forwarding of chain messages is not permitted.
Staff should not use personal email accounts for sending sensitive school information.
The official school email service may be regarded as safe and secure and is logged.
Users need to be aware that email communications may be monitored.
Users must immediately report, to the nominated person – in accordance with the school policy, the receipt of any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature and must not respond to any such email.
Any digital communication between staff and pupils or parents/carers must be professional in tone and content.
Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.
Spam, phishing and virus attachments can make email dangerous. The school ICT provider ensures mail is virus checked (ingoing and outgoing), includes spam filtering and backs emails up daily.

Emailing Personal, Sensitive, Confidential or Classified Information (GDPR)

Assess whether the information can be transmitted by other secure means before using e-mail - e-mailing confidential data is not recommended and should be avoided where possible;
The use of personal email accounts (e.g. Hotmail, BTInternet, AOL or any other Internet based webmail service) for sending sensitive information is not permitted.

Where your conclusion is that e-mail must be used to transmit such data:
Obtain express consent from your manager to provide the information by e-mail;
Exercise caution when sending the e-mail and always follow these checks before releasing the e-mail:
Verify the details, including accurate e-mail address, of any intended recipient of the information;
Verify (by phoning) the details of a requestor before responding to e-mail requests for information;
Do not copy or forward the e-mail to any more recipients than is absolutely necessary.
Do not send the information to any person whose details you have been unable to separately verify (usually by phone);
Send the information as an encrypted e-mail via Flowcrypt;
Provide the encryption key or password by a **separate** contact with the recipient(s);
Do not identify such information in the subject line of any e-mail.

Zombie Accounts

Zombie accounts refers to accounts belonging to users who have left the school and therefore no longer have authorised access to the school's systems. Such Zombie accounts when left active can cause a security threat by allowing unauthorised access.
Ensure that all user accounts are disabled once the member of the school community has left.

Managing Published Content

The contact details on the website should be the school address, email and telephone number. Staff or pupils' personal information must not be published.
The head teacher will take overall editorial responsibility for online content published by the school and will

ensure that content published is accurate and appropriate.
The school website will comply with the school's guidelines for publications including respect for intellectual property rights, privacy policies and copyright.

Use of Digital and Video Images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and students/pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff, students/pupils and parents/carers need to be aware of the risks associated with sharing images and with posting digital images on the internet. Those images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. There are many reported incidents of employers carrying out internet searches for information about potential and existing employees. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

When using digital images, staff and parents should be aware of the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.
Staff are allowed to take digital/video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should normally be taken on school equipment; **however, the use of personal equipment of staff can be used for such purposes provided the photo/video is deleted upon uploading to the online destination (Flickr/Vimeo/Wordpress etc.).**
Care should be taken when taking digital/video images that students/pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
Photographs published on the website, or elsewhere that include students/pupils will be selected carefully and will comply with good practice guidance on the use of such images
Students'/Pupils' full names will not be used anywhere on a website, particularly in association with photographs.
Written permission from parents or carers will be obtained before photographs / videos of pupils are used.
Pupil's work can only be published with the permission of the student/pupil and parents or carers.

Managing Social Networking, Social Media and Personal Publishing Sites

The school will control access to social media and social networking sites.
Pupils will be advised never to give out personal details of any kind which may identify them and / or their location. Examples would include real name, address, mobile or landline phone numbers, school attended, IM and email addresses, full names of friends/family, specific interests and clubs etc.
Personal publishing and online communication will be taught via age appropriate sites that are suitable for educational purposes. They will be moderated by the school.
All members of the school community are advised not to publish specific and detailed private thoughts, especially those that may be considered threatening, hurtful or defamatory.
Newsgroups will be blocked unless a specific use is approved.
Concerns regarding pupils' use of social networking, social media and personal publishing sites (in or out of school) will be raised with their parents/carers, particularly when concerning students' underage use of sites.
Staff personal use of social networking, social media and personal publishing sites will be discussed as part of staff induction and outlined in the school Staff/Governor/Student (trainee) Acceptable Use Policy – see Appendix B.
Further guidance can be found in the links in Appendix C – 'Online Communication Code of Conduct for Staff Working with Children' and the 'Safe Use of Facebook and Other Social Networking Sites'.
A sample advice leaflet for parents on Social Networking Sites, in particular, Facebook, has been produced to help parents understand the dangers they and their children face online.

Managing Filtering

The school's broadband access includes a cloud filtering solution, called TrustNET supplied and maintained by Atomwide as part of the London Grid for Learning offer with Virgin Media. The regular update and maintenance

of the filtering is conducted in school by Steve Sinnott (Pentre Tech).
The school will have a clear procedure for reporting breaches of filtering. All members of the school community (all staff and all pupils) will be aware of this procedure.
If staff or pupils discover unsuitable sites, the URL will be reported to the School e-Safety Coordinator who will then record the incident and escalate the concern as appropriate (see Appendix D)
The School filtering system will block all sites on the Internet Watch Foundation (IWF) list.
The e-safety coordinator will ensure that regular checks are made to ensure that the filtering methods selected are effective.
Any material that the school believes is illegal will be reported to appropriate agencies such as IWF, Merseyside Police or CEOP.

Managing Videoconferencing

Currently the school does not use video conferencing equipment, should this change this document will be updated.

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.

General Data Protection Regulation

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 which states that personal data must be:

Fairly and lawfully processed;
Processed for limited purposes;
Adequate, relevant and not excessive;
Accurate;
Kept no longer than is necessary;
Processed in accordance with the data subject's rights;
Secure;
Only transferred to others with adequate protection.

More detailed information can be found in the School Data Protection Policy.

Staff must ensure that they:
At all times take care to ensure the safekeeping of personal data, minimising the risk of its loss or misuse.
Use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data.

Transfer data using encryption and secure password protected devices.

Disposal of Redundant ICT Equipment

Any redundant PCs will have hard drives destroyed.

All redundant ICT equipment will be disposed of through an authorised agency. This should include a written receipt for the item including an acceptance of responsibility for the destruction of any personal data.
All redundant ICT equipment that may have held personal data will have the storage media over written multiple times to ensure the data is irretrievably destroyed. Or if the storage media has failed it will be physically destroyed. We will only use authorised companies who will supply a written guarantee that this will happen.

Disposal of any ICT equipment will conform to:
The Waste Electrical and Electronic Equipment Regulations 2006
The Waste Electrical and Electronic Equipment (Amendment) Regulations 2007
Environment Agency Guidance (WEEE)
ICO Guidance - Data Protection Act 1998
Electricity at Work Regulations 1989

The school will maintain a comprehensive inventory of all its ICT equipment including a record of disposal.

The school's disposal record will include:
Date item disposed of;
Authorisation for disposal, including:
Verification of software licensing
Any personal data likely to be held on the storage media? *
How it was disposed of e.g. waste, gift, sale
Name of person and/or organisation who received the disposed item
If personal data is likely to be held the storage media will be overwritten multiple times or "scrubbed" to ensure the data is irretrievably destroyed.

Policy Decisions

Authorising Internet Access

All staff will read and sign the Staff/Governor/Student (trainee) Acceptable Use Policy (Appendix B) before using any school ICT resources.
Parents will be asked to read and sign the School Acceptable Use Policy for pupil access (Appendix A) and discuss it with their child, where appropriate.
All visitors to the school site who require access to the schools network or internet access will be asked to read and sign the Staff/Governor/Student (trainee) Acceptable Use Policy (Appendix B).
Parents will be informed that pupils will be provided with supervised Internet access appropriate to their age and ability.
When considering access for vulnerable members of the school community (such as with children with special education needs) the school will make decisions based on the specific needs and understanding of the pupil(s*).*

According to Setting Type:
Pupils' access to the Internet will be by adult demonstration and teacher directed independent work using specific and approved online materials.

Assessing Risks

The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the global and connected nature of Internet content, it is not possible to guarantee that access to unsuitable material will never occur via a school computer. Neither the school nor the LA can accept liability for the material accessed, or any consequences resulting from Internet use.
The school will audit ICT use to establish if the e–Safety policy is adequate and that the implementation of the e–safety policy is appropriate – see Appendix E for a School e-Safety Audit proforma.
The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990 and breaches will be reported to Merseyside Police.
Methods to identify, assess and minimise risks will be reviewed regularly.

Unsuitable/Inappropriate Activities

The school believes that the activities referred to in the following section would be inappropriate in a school context and that users, as defined below, should not engage in these activities in school or outside school when using school equipment or systems. The school policy restricts certain internet usage as follows:

Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:

child sexual abuse images
promotion or conduct of illegal acts, e.g. under the child protection, obscenity, computer misuse and fraud legislation
adult material that potentially breaches the Obscene Publications Act in the UK
criminally racist material in UK
pornography
promotion of any kind of discrimination
promotion of racial or religious hatred
threatening behaviour, including promotion of physical violence or mental harm
any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute
Using school systems to run a private business
Use systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school
Uploading, downloading or transmitting commercial software or any copyrighted materials belonging to third parties, without the necessary licensing permissions
Revealing or publicising confidential or proprietary information (e.g. financial/personal information, databases, computer/network access codes and passwords)
Creating or propagating computer viruses or other harmful files
Carrying out sustained or instantaneous high volume network traffic (downloading/uploading files) that causes network congestion and hinders others in their use of the internet
On-line gambling
On-line shopping/commerce
File sharing

Responding to Incidents of Concern

If any apparent or actual misuse appears to involve illegal activity i.e.

- child sexual abuse images
- adult material which potentially breaches the Obscene Publications Act
- criminally racist material
- other criminal conduct, activity or materials

All members of the school community will be informed about the procedure for reporting e-Safety concerns (such as breaches of filtering, cyberbullying, illegal content etc.).
The e-Safety Coordinator will record all reported incidents and actions taken in the School e-Safety incident log and other in any relevant areas e.g. Bullying or Child protection log.
The Designated Person for Child Protection will be informed of any e-Safety incidents involving Child Protection concerns, which will then be escalated appropriately – See Child Protection Policy for dealing with concerns.
The school will manage e-Safety incidents in accordance with the school discipline/behaviour policy where appropriate.
The school will inform parents/carers of any incidents of concerns as and when required.
After any investigations are completed, the school will debrief, identify lessons learnt and implement any changes required.
Where there is cause for concern or fear that illegal activity has taken place or is taking place then the school will contact Children's Services and escalate the concern to the Police.
Any racist incidents will be reported to Children's Services. Racist Incident Monitoring forms should be completed electronically through the School Portal. This allows for individual incidents to be reported as and when they happen and will also generate a termly report for schools to agree to and return.
If the school is unsure how to proceed with any incidents of concern, then the incident may be escalated to the Local Authority Designated Officer (LADO) – see Child Protection Policy.

If members of staff suspect that misuse might have taken place, but that the misuse is not illegal (as above) it is essential that correct procedures are used to investigate, preserve evidence and protect those carrying out the investigation. More than one member of staff should be involved in the investigation which should be carried out on a "clean" designated computer.

It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour/disciplinary procedures

Handling e–safety Complaints

- Complaints about Internet misuse will be dealt with under the School's complaints procedure.

- Any complaint about staff misuse will be referred to the head teacher.

- All e–safety complaints and incidents will be recorded by the school, including any actions taken (see Appendix I).
- Pupils and parents will be informed of the complaints procedure.
- Parents and pupils will need to work in partnership with the school to resolve issues.
- 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.
- Discussions will be held with the local Police and/or Children's Services to establish procedures for handling potentially illegal issues.
- 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.

How the Internet is used across the Community

- The school will be sensitive to Internet-related issues experienced by pupils out of school, e.g. social networking sites, and offer appropriate advice.
- The school will provide appropriate levels of supervision for pupils who use the internet and technology whilst on the school site.
- The school will provide an AUP for any guest who needs to access the school computer system or internet on site.

Managing Cyber-bullying:

The use of technology has become a significant component of many safeguarding issues, for example, technology often provides the platform that facilitates child sexual exploitation, criminal exploitation, radicalisation and sexual predation.

There are three categories of risk:
Content: being exposed to illegal, inappropriate or harmful material, for example, pornography, fake news, racist or radical and extremist views;
Contact: being exposed to harmful online interaction with other users, for example, commercial advertising as well as adults posing as children or young adults; and
Conduct: personal online behaviour that increases the likelihood of, or causes, harm, for example, making, sending and receiving explicit images, or online bullying.
Cyber-bullying (along with all other forms of bullying) of any member of the school community will not be tolerated.

There are clear procedures in place to support anyone in the school community affected by online bullying.
All incidents of cyber-bullying reported to the school will be recorded and investigated.
The school will take steps to identify the perpetrator, where possible and appropriate. This may include examining school system logs, evidence from pupils/parents, identifying and interviewing possible witnesses, and contacting the service provider and the police, if necessary.
Pupils, staff and parents/carers will be required to work with the school to support the approach to online bullying and the school's e-Safety ethos.

Sanctions for those involved in online bullying may include:
The perpetrator 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. Other sanctions for pupils and staff may also be used in accordance with the Behaviour Policy, Acceptable Use Policy and Disciplinary Procedures.
Parent/carers of pupils will be informed.
The Police will be contacted if a criminal offence is suspected.

Managing Learning Environment/Platforms:

With any online resource, care must be taken to protect pupils' data and passwords as much as possible.
All pupils will be inducted into the safe use of the VLE as part of their first session using any VLE platform.
If a pupil's account is compromised, all efforts will be taken to reset passwords and inform parents if the need arises. For any breach of security regarding the VLEs, the incident log may be used in appendix D.

Managing Mobile Phones and Personal Devices:

The use of mobile phones and other personal devices by staff and students in school will be decided by the school and covered in the school Acceptable Use Policies.
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 discipline/behaviour policy.
Pupils are not allowed to use phones at school and are discouraged from bringing them onto the school site. If a pupil does bring a phone to school it will be kept safe by the class teacher until the end of the school day when pupils can collect it.
Staff and student mobile phones and personal devices will not be used during lessons or formal school time. They should be switched off or left on silent in the staff cupboards.
In the case of an emergency, permission can be sought from the headteacher to keep a mobile phone close at hand.
The Bluetooth function of a mobile phone should not be used to send school images or school files to other mobile phones.
Electronic devices of all kinds that are brought in to 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.

Pupils 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/carers in accordance with the school policy.
If a pupil needs to contact his/her parents/carers they will be allowed to use the main office school phone. Parents are advised not to contact their child via their mobile phone during the school day, but to contact the school office.

Staff use of personal devices:

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 must use a school phone where contact with pupils or parents/carers is required.
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 the headteacher or SMT in emergency circumstances.
Staff will not ordinarily 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. However, when photos or videos are taken on personal devices, the digital file should be **completely deleted** from the device as soon as the file has been uploaded to its online destination (e.g. Flickr, Vimeo, Wordpress etc.)
Staff working in EYFS may only use personal devices whilst away from the school premises (e.g. an educational visit), to upload photos to the class blog with the clear understanding that as soon as the photo has been uploaded, that it is **completely deleted**.
If a member of staff breaches the school policy then disciplinary action may be taken.

Communication Technologies

Mobile phones may be brought to school by pupils in Upper Key Stage 2 only (Years 5 & 6) and must be switched off and handed to staff on arrival.
Use of mobile phones in lessons is not allowed without seeking express permission beforehand.
Use of mobile phones in social time is allowed for staff; no pupil use of mobile phones whilst on site.
Taking photos on mobile phones or other camera devices is allowed for staff, adhering to the ground rules as set out above; not allowed for pupils.
Use of personal hand held devices e.g. PDAs, PSPs is not allowed without seeking express **permission beforehand.**
Use of personal email addresses in school, or on school network
Use of school email for personal emails is not allowed.
Use of chat rooms/facilities are not allowed.
Use of instant messaging is not allowed.
Use of social networking sites Use of blogs for educational purposes is allowed and positively encouraged

Communication of Policy

Introducing the Policy to Pupils?

Think U Know: www.thinkuknow.co.uk
Childnet: www.childnet.com
Kidsmart: www.kidsmart.org.uk
Orange Education: www.orange.co.uk/education
Safe: www.safesocialnetworking.org

All users will be informed that network and Internet use will be monitored.
An e–safety training programme will be established across the school to raise the awareness and importance of safe and responsible internet use amongst pupils.
Pupil instruction regarding responsible and safe use will precede Internet access.
An e–safety module will be included in the school curriculum and reinforced throughout the year.
e–safety will be part of the transition programme when moving between establishments.
e-Safety rules will be posted in all rooms with Internet access.
Particular attention to e-Safety education will be given where pupils are considered to be vulnerable.

Discussing the Policy with Staff

The e–safety Policy will be formally provided to and discussed with all members of staff.
To protect all staff and pupils, the school will implement Acceptable Use Policies.
Staff will be made aware that Internet traffic can be monitored and traced to the individual user.
Discretion and professional conduct is essential.

Up-to-date and appropriate staff training in safe and responsible Internet use, both professionally and personally, will be provided for all members of staff.
The School will highlight useful online tools which staff should use with children in the classroom. These tools will vary according to the age and ability of the pupils.
All members of staff will be made aware that their online conduct out of school could have an impact on their role and reputation within school. Civil, legal or disciplinary action could be taken if they are found to bring the profession or institution into disrepute, or if something is felt to have undermined confidence in their professional abilities.

Enlisting Parents' Support

Parents' attention will be drawn to the school e–safety Policy in newsletters, the school prospectus and on the school website.
A partnership approach to e-Safety at home and at school with parents will be encouraged.
Parents will be encouraged to read and sign the school Acceptable Use Policy for pupils and discuss its implications with their children.
Information and guidance for parents on e–safety will be made available to parents in a variety of formats.
Advice on useful resources and websites, filtering systems and educational and leisure activities which include responsible use of the Internet will be made available to parents.
At least one parent with an active interest in ICT will be part of the e-safety working party.

APPENDIX A

PUPIL ACCEPTABLE USE POLICY / AGREEMENT

English Martyrs Catholic Primary School

These rules will help us to be fair to others and keep everyone safe.

- I will only use ICT in school for school purposes.
- I will only open/delete my own files.
- I will make sure that all ICT contact with other children and adults is responsible, polite and sensible.
- I will not deliberately look for, save or send anything that could be unpleasant or nasty. If I accidentally find anything like this I will click on the **CEOP Report Abuse** button and/or tell my teacher immediately.
- I will not give out my own details such as my name, phone number or home address. When using the internet at school or at home. I will not arrange to meet someone unless my parents have agreed.
- I will be responsible for my behaviour when using ICT because I know that these rules are to keep me safe.
- Myself and my family will support the school approach to online safety and not deliberately upload or add any images, video, sounds or text that could upset any member of the school community.
- I know that my use of ICT can be checked and that my parent/carer contacted if a member of school staff is concerned about my e-Safety.

Pupil Acceptable Use - Parent/Carer Agreement

Dear Parent/ Carer,

ICT including the internet, e-mail and mobile technologies, etc. has become an important part of learning in our school. We expect all children to be safe and responsible when using any ICT.
Please read and discuss these e-Safety rules with your child and return the slip at the bottom of this page. If you have any concerns or would like some explanation please contact **Mr Roach.**

Parent/Carer signature

We have discussed this and ..... (child name) agrees to follow the e-Safety rules and to support the safe use of ICT at **English Martyrs Catholic Primary** School.

Parent/Carers Name		**Pupil Class**	
Signed *(Parent/Carer)*		**Date**	

APPENDIX B

STAFF / GOVERNOR/ STUDENTS (trainee)
ACCEPTABLE USE POLICY AGREEMENT

English Martyrs Catholic Primary School

ICT (including data) and the related technologies such as e-mail, 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 ICT. This applies to ICT used in school and also applies to use of school ICT systems and equipment out of school and use of personal equipment in school or in situations related to their employment by the school. All staff/Governors/visitors are expected to sign this policy and adhere at all times to its contents. Any concerns or clarification should be discussed with **Paul Roach** (e-Safety coordinator) or **Lewis Dinsdale** (Head teacher).

- I will only use the school's email/Internet/Intranet and any related technologies for professional purposes or for uses deemed 'reasonable' by the Head teacher or Governing Body.
- I will comply with the ICT 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 e-mail address to parents or pupils.
- I will only use the approved, secure e-mail system(s) for any school business.
- I will ensure that personal data (such as data held on SIMS software) 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 teacher or Governing Body. Personal or sensitive data taken off site must be encrypted.
- I will not install any hardware of software without permission of **Paul Roach.**
- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.
- Images of pupils and/or staff will only be taken, stored and used for professional purposes using school equipment 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 Head teacher.
- I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available, on request, to my Head teacher.
- I will support the school approach to online safety and not deliberately upload or add any images, video, sounds or text that could upset or offend any member of the school community.
- 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 e-Safety, Data Protection and Behaviour policies and help pupils to be safe and responsible in their use of ICT and related technologies.
- I understand this forms part of the terms and conditions set out in my contract of employment.
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action.

Staff / Governor / Student - Acceptable Use Agreement

Name			
Job Title			
Signed		**Date**	

I have read and understand the above and agree to use the school ICT systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines. I agree to follow this code of conduct and to support the safe and secure use of ICT throughout the school.

APPENDIX C

E-SAFETY LINKS

The following links may help those who are developing or reviewing a school e-Safety policy.

- **CEOP (Child Exploitation and Online Protection Centre)**: Click here to access
- **Childline**: Click here to access
- **Childnet**: Click here to access
- **Click Clever Click Safe Campaign**: Click here to access
- **Cybermentors**: Click here to access
- **Digizen**: Click here to access
- **Internet Watch Foundation (IWF)**: Click here to access
- **Kidsmart**: Click here to access
- **Teach Today**: Click here to access
- **Think U Know website**: Click here to access
- **Virtual Global Taskforce — Report Abuse**: Click here to access
- **Orange Education**: Click here to access
- **Safe**: Click here to access
- **Information Commissioner's Office (ICO)** Click here to access
- **INSAFE** Click here to access
- **National Education Network (NEN)** E-Safety Audit Tool: Click here to access
- **Anti-Bullying Network** - Click here to access
- **Cyberbullying.org** - Click here to access
- **Ofcom Report:** Click here to access
- **Learning Curve Education:** Click here to access
- **UK Safer Internet Centre:** Click here to access
- **UK Council for Child Internet Safety (UKCCIS):** Click here to access
- **Wise Kids:** Click here to access
- **Teacher Tube:** Click here to access
- **Teach Today:** Click here to access
- **Beat Bullying:** Click here to access
- **BBC Teachers:** Click here to access
- **Grid Club**: Click here to access
- **Teem:** Click here to access
- **Sites for Teachers:** Click here to access
- **DfE:** Click here to access
- **Know the Net:** Click here to access
- **Family Online Safety Institute:** Click here to access
- **e-safe Education**: Click here to access
- **Facebook Advice to Parents:** Click here to access
- **Record Management Society:** Click here to access
- **Test your online safety skills:** Click here to access

APPENDIX D

ENGLISH MARTYRS CATHOLIC PRIMARY SCHOOL - E-SAFETY INCIDENT LOG

Details of e-Safety incidents to be recorded by the e-Safety Coordinator. This incident log will be monitored termly by the Head teacher, member of SLT or Chair of Governors.

Date	Time	Name of Pupil or Staff Member	Male or Female	Room and Computer/ Device No.	Details of Incident (including Evidence)	Actions and Reasons

Reviewed:	September 2018	Reviewed by:	L. Dinsdale, P. Roach	Status:	Active
Date Agreed:	21st Sept 2018	Next Review:	September 2019		