ST. WINEFRIDE'S CATHOLIC PRIMARY SCHOOL

E-Safety Policy

Mission Statement

Welcome to St Winefride's where we come together to learn, laugh, listen, live and love in the presence of Jesus.

At our school, we believe that everyone is valued as a unique gift from God.

We work together to create an engaging learning environment, where all children are challenged to achieve their full potential.

Rationale

New technologies inspire children to be creative, communicate and learn. However, while the internet is a great resource, it is important that children and young people are protected from the risks they may encounter. St. Winefride's Catholic Primary School endeavours to highlight benefits and risks of using technology and provides Safeguarding and education for users to enable them to control their online experience.

The following local/national guidance should also be read in conjunction with this policy:

- Cheshire Local Safeguarding Children Partnership, Guidelines and Procedures (2019)
- PREVENT Strategy HM Government
- Keeping Children Safe in Education DfE September 2023
- Teaching Online Safety in Schools DfE June 2019
- Working together to Safeguard Children
- Learning together to be Safe: A Toolkit to help Schools contribute to the Prevention of Violent Extremism.

The Internet and other digital and information technologies are powerful tools, which open up new opportunities for everyone. Electronic communication helps teachers and pupils learn from each other. These technologies can stimulate discussion, promote creativity and increase awareness of context to promote effective learning. Pupils 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.

Why is Internet Use Important?

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 information and administration systems.

Internet use is part of the statutory curriculum and a necessary tool for learning. It is an essential element in 21st century life for education, business and social interaction. Access to the Internet is therefore an entitlement for

pupils who show a responsible and mature approach to its use. Our school has a duty to provide pupils with quality Internet access.

Pupils will use the Internet outside school and will need to learn how to evaluate Internet information and to take care of their own safety and security.

How does Internet Use Benefit Education?
Benefits of using the Internet in education include:

- access to world-wide educational resources including museums and art galleries
- educational and cultural exchanges between pupils world-wide
- 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 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 Cheshire West and Chester and DFE
- access to learning wherever and whenever convenient.

The use of these exciting and innovative tools in school and at home has been shown to raise educational standards and promote pupil / student 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, unsuitable video / Internet games,
- 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,
- An inability to evaluate the quality, accuracy and relevance of information on the Internet,
- The potential for excessive use which may impact on the social and emotional development and learning of the young person.

As with all other risks, it is impossible to eliminate those risks completely. It is therefore essential, through good educational provision to build 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.

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

- Responsible ICT use by all staff and pupils; 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 from the London Grid for Learning including the effective management of content filtering.
- National Education Network standards and specifications.

Learning and Teaching

We believe that the key to developing safe and responsible behaviours online, not only for pupils but everyone within our school community, lies in effective education. We know that the internet and other technologies are embedded in our pupils' lives, not just in our school but outside as well, and we believe we have a duty to help prepare our pupils to safely benefit from the opportunities the internet brings.

We will provide a curriculum/other lessons which has e-Safety related lessons embedded throughout.

- Internet access will be planned to enrich and extend learning activities.
- School will celebrate and promote e-Safety through assemblies and whole-school activities, including promoting Safer Internet Day.
- We will discuss, remind or raise relevant e-Safety messages with pupils routinely wherever suitable opportunities arise during all lessons; including the need to protect personal information, consider the consequences their actions may have on others, the need to check the accuracy and validity of information they use and the need to respect and acknowledge ownership of digital materials.
- Any internet use will be carefully planned to ensure that it is age appropriate, supporting the learning objective for specific curriculum areas and includes filtering appropriate to the age of pupils, through the local authority.
- Pupils will be taught how to use a range of age-appropriate online tools in a safe and effective way. They will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.
- We will remind pupils about their responsibilities through an Acceptable Use Policy which every pupil will sign and be displayed throughout the school.
- School will model safe and responsible behaviour in their own use of technology during lessons.
- We will teach pupils how to search for information and to evaluate the content of websites for accuracy when using them in any curriculum area.
- When searching the internet for information, pupils will be guided to use age-appropriate search engines. All use will be monitored, and pupils will be reminded of what to do if they come across unsuitable content.
- Pupils will be taught about the impact of online bullying and know how to seek help if they are affected by any form of online bullying. See Anti-Bullying Policy.
- Pupils will be made aware of where to seek advice or help if they experience problems when using the internet and related technologies, i.e. parent or carer, teacher or trusted staff member, or an organisation such as Childline.

Managing ICT Systems and Access

- All users will sign an Acceptable Use Policy provided by the school, appropriate to their age and type of access. Users will be made aware that they must take responsibility for their use and behaviour while using the school ICT system and that such activity will be monitored and checked.
- Emerging technologies will be examined for educational benefit and, if need be, a risk assessment will be carried out before use in school is allowed.
- At Key Stage 1, pupils will access the network using an individual username and a class password which the teacher supervises.
- At Key Stage 2, pupils will have an individual user account with an appropriate password which will be kept secure, in line with the pupil Acceptable Use Policy. They will ensure that they log out after each session.
- All internet access will be undertaken alongside a member of staff or, if working independently, a member of staff will supervise at all times.
- Members of staff will access the internet using an individual ID and password, which they will keep secure. They will ensure that they log out after each session and not allow pupils to access the internet through their ID or password. They will abide by the school AUP at all times.

- Staff should not use personal mobile phones to take photographs or videos of children. Staff should only use school mobile phone or digital camera. Mobile phones are not permitted for use anywhere in school, around the children. This applies to members of staff and other visitors to the school. Mobile phones may only be used in office areas, staffroom etc. The only exception to this is staff taking a mobile phone with them on a school visit outside of school, for use in emergencies only.

Managing Filtering

- The school has the Smoothwall filtering system in place which is managed by the school and the local authority. Banned phrases and websites are identified.
- The school has a clearly defined procedure for reporting breaches of filtering. All staff and pupils will be aware of this procedure by reading and signing the Acceptable Use Policy and by attending the appropriate awareness training/online safety lesson
- If staff or pupils discover an unsuitable site, it must be reported to a member if the Senior Leadership Team immediately. The school will report content and any relevant details to the Local Authority helpdesk via the Online safety coordinator or network manager.
- Any amendments to the school filtering policy or block and allow lists will be checked and assessed by the headteacher/e-Safety Co-ordinator prior to being released or blocked.
- The evaluation of online content materials is a part of teaching and learning in every subject and will be viewed as a whole-school requirement across the curriculum. Pupils should be taught to be critically aware of the materials they are shown and how to validate information before accepting its accuracy.

Email

- Pupils may only use approved e-mail accounts allocated to them by the school and should be aware that any use of the school email system will be monitored and checked.
- Pupils are encouraged to immediately tell a teacher or trusted adult if they receive any inappropriate or offensive emails
- Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.
- Whole class or group e-mail addresses should be used in school
- E-mail sent to external organisations should be written carefully and authorised before sending, in the same way as a letter written on school headed paper.
- Chain messages are not permitted or forwarded on to other school owned email addresses.
- Staff should not use personal email accounts for professional purposes, especially to exchange any school related information or documents or to email parents/carers.
- Staff should not send emails to pupils.
- Irrespectively of how pupils or staff access their school email (from home or within school), school policies still apply.

Social Networking

- Staff will not post content or participate in any conversations which will be detrimental to the image of the school. Doing so will result in disciplinary action and, in certain situations, could result in dismissal.
- Staff who hold social media accounts are advised not have parents as their 'friends'.
- Staff should never have pupils as 'friends'. This will be regarded as a safeguarding issue and will result in disciplinary action and, in certain situations, could result in dismissal
- Access to social media/networking sites and newsgroups is blocked on school equipment but can be accessed by staff and parents off-site. The only exception to this is the school mobile phones.

- Pupils will be advised never to give out personal details of any kind which may identify them or their location.
- Pupils should be advised not to place personal photos on any social network space.
- Pupils should be advised on security and encouraged to set passwords, deny access to unknown individuals and instructed how to block unwanted communications. Pupils should be encouraged to invite known friends only and deny access to others.

Publishing Content Online

- The contact details on the Web site will only be the school address, e-mail and telephone number. Staff or pupils' personal information will not be published.
- The headteacher or Admin Officer will take overall editorial responsibility and ensure that content is accurate and appropriate.
- Pupils will not be allowed to post or create content on sites unless the site has been approved by a member of the teaching staff.
- Pupils' full names will not be used anywhere on the website, particularly in association with photographs and video.
- Written permission is obtained from the parents/carers before photographs and videos are published.
- Any images, videos or sound clips of pupils must be stored on the school network and never transferred to personally-owned equipment.
- Pupils and staff are not permitted to use portable devices to store images/video/sound clips of pupils.

Mobile Phones and Devices

General use of personal devices

- Staff must not use personal mobile phones and other electronic devices in any way during lessons time.
- Staff must not use personal devices such as mobile phones or cameras to take photos or videos of pupils and will only use school provided equipment for this purpose.
- Mobile phones and personally-owned devices should be switched to 'silent' mode and not be used during teaching periods unless permission has been granted by a member of the senior leadership team in emergency circumstances
- In the case of school productions, parents/carers are permitted to take photographs of their child in accordance with school protocols, which advises parents/carers not to publish photographs of other children on the photograph without permission of the other child/children's parents/carers.
- The sending of abusive or inappropriate text, picture or video message is forbidden.

Pupils' use of personal devices

- Pupils who bring their own mobile phones into school are required to hand them in to their class teacher every morning and devices are collected at home time. This applies only to older children (year 5 and 6) who walk to and from school alone. The school will not be held liable for loss of mobile phones.
- Pupils who do not follow the school policy relating to the use of mobile phones will not be permitted to bring their mobile phones into school.

Screening, Searching and Confiscation - The Education Act 2011, allows staff to lawfully search electronic devices, without consent or parental permission, if there is a suspicion that the pupil has a device prohibited by school rules, or the staff member has good reason to suspect the device may be used to:

- cause harm

- disrupt teaching
- break school rules
- commit an offence
- cause personal injury
- damage property.

CCTV

- The school uses CCTV in some areas of school property as a security measure.
- Cameras will only be used in appropriate areas and there is clear signage indicating where it is in operation.

General Data Protection (GDPR) and e-safety

Data must always be processed lawfully, fairly and transparently; collected for specific, explicit and legitimate purposes; limited to what is necessary for the purposes for which it is processed; accurate and kept up to date; held securely; only retained for as long as is necessary for the reasons it was collected.

GDPR is relevant to e-safety since it impacts on the way in which personal information should be secured on school networks, computers and storage devices; and the security required for accessing, in order to prevent unauthorised access and dissemination of personal material.

Staff need to ensure that care is taken to ensure the safety and security of personal data regarding all of the school population and external stakeholders, particularly, but not exclusively: pupils, parents, staff and external agencies. Personal and sensitive information should only be sent by e mail when on a secure network. Personal data should only be stored on secure devices.

In the event of a data breach, the school will notify the Trust's Data Protection Officer (DPO) immediately, who may need to inform the Information Commissioner's Office (ICO).

Authorising Internet access

- All staff must read and sign the 'Acceptable Use Policy' before using any of school ICT resources.
- All parents will be required to sign the home-school agreement prior to their children being granted internet access within school.
- All visitors and students will be asked to read and sign the Acceptable User Policy prior to being given internet access within the school.
- The school will maintain a current record of all staff and pupils who have been granted access to the school's internet provision.

Support for Parents

- Parents attention will be drawn to the school's e-Safety policy and safety advice in newsletters, the school website and e-Safety information workshops.
- The school website will be used to provide parents with timely and meaningful information about their children's school lives and work to support the raising of achievement. The website will also provide links to appropriate online-safety websites.

Radicalisation Procedures and Monitoring

It is important for us to be constantly vigilant and remain fully informed about the issues which affect the region in which we teach. Staff are reminded to suspend any professional disbelief that instances of radicalisation 'could

not happen here' and to refer any concerns through the appropriate channels (currently via the Child Protection/Safeguarding Lead). Regular monitoring and filtering is in place to ensure that access to appropriate material on the internet and key word reporting it in place to ensure safety for all staff and pupils.

Sexual Harassment
Sexual harassment is likely to: violate a child's dignity, make them feel intimated, degraded or humiliated and/or create a hostile, offensive or sexualised environment.

Online sexual harassment, which might include non-consensual sharing of sexual images and videos and sharing sexual images and videos (both often referred to as 'sexting'; inappropriate sexual comments on social media; exploitation; coercion and threats).

Any reports of online sexual harassment will be taken seriously, and the police and Children's Social Care may be notified. Our school follows and adheres to the national guidance'

Responses to Incident of Concern
An important element of e-Safety is the ability to identify and deal with incidents of concern including the confidentiality of information. All staff, volunteers and pupils have a responsibility to report e-Safety incidents or concerns so that they may be dealt with effectively and in a timely manner in order to minimise any impact. The school has incident reporting procedures in place and record incidents of an e-Safety nature on CPOMs.

Sanctions
Misuse of the Internet may result in disciplinary action, including written warnings, withdrawal of access privileges, and in extreme cases, suspension or expulsion, in accordance with the school's Behaviour or Discipline Policy. The school also reserves the right to report any illegal activities to the appropriate authorities

Handling E-Safety Complaints

- Complaints of internet misuse will be dealt with by a senior leader.
- Any complaint re/staff misuse will be referred to the headteacher.
- Complaints of a child protection nature will be dealt with in accordance with school Safeguarding procedures.
- In the case of any potential illegal usage, police advice will be sought.

Communication of Policy

Pupils

- Rules for Internet access will be shared with pupils.
- Pupils will be informed that Internet use will be monitored.

Staff

- This E-Safety Policy will be shared with staff.
- Staff training in Safeguarding procedures, will include elements of E-Safety and The Prevent Duty.
- Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.

Parents

- Parents' attention will be drawn to the E-Safety Policy in newsletter and on the school Web site. The school will also organise E safety workshops to support parents' understanding of how to best safeguard their children against potential online dangers.

Roles and Responsibilities

Headteacher and Senior Leaders are responsible for:

- Ensuring the safety (including e-Safety) of members of the school community and the day to day responsibility,
- Ensuring that relevant staff receive suitable CPD to enable them to carry out their e-Safety roles,
- Knowing the procedures to be followed in the event of a serious e-Safety allegation being made against a member of staff.

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,
- Signing the school Staff Acceptable Use Policy,
- Reporting any suspected misuse or problem to the appropriate person for investigation,
- Ensuring that digital communications with pupils (e-mail / website) should be on a professional level and only carried out using official school communication systems,
- Ensuring that e-Safety issues are embedded in all aspects of the curriculum and other school activities,
- Ensuring that pupils understand and follow the school e-Safety and acceptable use policy,
- Monitoring ICT activity in lessons, extra-curricular and extended school activities,
- Being aware of e-Safety issues related to the use of mobile phones, cameras and hand held devices and that they monitor their use and implement current school policies with regard to these devices,
- Guide pupils 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 and Deputy Lead - Staff 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,
- cyber-bullying.

Students / pupils

- Are responsible for using the school ICT systems in accordance with the Pupil Acceptable Use Policy,
- Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so,
- Will be expected to know and understand school policies on the use of mobile phones, digital cameras and hand held devices. They should also know and understand school policies on the taking / use of images and on cyber-bullying,
- should understand the importance of adopting good e-Safety practice when using digital technologies out of school.

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. The school will therefore take every opportunity to help parents understand these issues through parents' evenings, newsletters, website / VLE and information about national / local e-Safety campaigns / literature. Parents and carers will be responsible for:

- endorsing (by signature) the Pupil Acceptable Use Policy,
- accessing the school website / on-line pupil records in accordance with the relevant school Acceptable Use Policy.

Staff Training

Our staff receive regular information and training on e-Safety issues, as well as updates as and when new issues arise.

- As part of the induction process all staff receive information and guidance on the e-safety policy , the school's Acceptable Use Policy , e-security and reporting procedures.
- All staff will be made aware of individual responsibilities relating to the safeguarding of children within the context of e-safety and know what to do in the event of misuse of technology by any member of the school community.
- All staff will be encouraged to incorporate e-Safety activities and awareness within their curriculum areas.

Links to other policies and national guidance

The following school policies and procedures should also be referred to

- Safeguarding Children Policy
- Whistleblowing Policy
- Behaviour Policy
- Anti-Bullying Policy
- Guidance on Safer Working Practice
- Staff code of conduct
- Data Protection/GDPR
- Acceptable Use Policy

Appendix 1

St. Winefride's Catholic Primary School

Information and Communications Technology

Acceptable use of Internet Agreement

Pupil and Parent Agreement

When I use the Internet and e-mail at school, I will keep to these rules:

- I will only use the Internet with permission, when there is a teacher or adult helper present.
- I will not try to find unsuitable sites on the Internet
- I will only e-mail people I know, or who my teacher has approved
- The messages I send will be polite and sensible
- I will not give my full name or home address or telephone number, or arrange to meet someone unless my parent, carer, or teacher has given permission.

Pupil's signature …….. **Date:** …….

Parent

As the parent or legal guardian of the pupil signing above, I give permission for my son or daughter to use electronic mail and the Internet, under supervision at school.

I understand and accept the above rules for acceptable use of the Internet and will discuss these with my child.

Parents' signature ……. **Date**……

Pupil's name ……

Class ……

Appendix 2

St. Winefride's Catholic Primary School

Staff Information Systems Code of Conduct

To ensure that staff are fully aware of their professional responsibilities when using information systems, they are asked to sign this code of conduct. Staff should consult the school's Online safety policy for further information and clarification.

- The information systems are school property and I understand that it is a criminal offence to use a computer for a purpose not permitted by its owner.

- I will ensure that my information systems use will always be compatible with my professional role.
- I understand that school information systems may not be used for private purposes, without specific permission from the headteacher.
- I understand that the school may monitor my information systems and Internet use to ensure policy compliance.
- I will respect system security and I will not disclose any password or security information to anyone other than an appropriate system manager.
- I will not install any software or hardware without permission.
- I will ensure that personal data is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely.
- I will respect copyright and intellectual property rights.
- I will report any incidents of concern regarding children's safety to the school the Safeguarding Lead or Deputy Safeguarding Lead.
- I will ensure that any electronic communications with pupils are compatible with my professional role.
- I will promote Online safety with pupils in my care and will help them to develop a responsible attitude to system use and to the content they access or create.

The school may exercise its right to monitor the use of the school's information systems, including Internet access, the interception of e-mail and the deletion of inappropriate materials where it believes unauthorised use of the school's information system may be taking place, or the system may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.

I have read, understood and agree with the Information Systems Code of Conduct.

Signed: …… Capitals: …… Date: ……

Accepted for school: …….. Capitals: ……