St. Peter's Catholic Academy
E-Safety Policy

"Together, One Family, One Community in Christ"

In the words of our children, our mission is...

To serve God together as one.
To show that we live the Gospel Values and Virtues together as one community.
To respect and love all in our community.
To love, work and play as part of God's family.
To put God first in our lives and become the people he wants us to be.

E-Safety Policy
E-Safety encompasses Internet technologies and electronic communications such as mobile phones as well as collaboration tools and personal publishing. It highlights the need to educate pupils about the benefits and risks of using technology and provides safeguards and awareness for users to enable them to control their online experience. Any previous Internet policy should be revised and renamed as the school's e Safety Policy to reflect the need to raise awareness of the safety issues associated with electronic communications as a whole. This policy applies to all members of the school community (including staff, students / pupils, volunteers, parents / carers, visitors, community users) who have access to and are users of school ICT systems, both in and out of the school.

The school's e-safety policy will operate in conjunction with other policies including those for Student Behaviour, Bullying, Curriculum, Data Protection and Security.

The C&YP Core e-Safety Policy
This core e-safety policy provides the essential minimal school e-safety policy and has been approved by the Children and Young People's Services(C&YP). C&YP considers that all the elements with a bullet are mandatory in order to protect users, the school and Stoke-on-Trent City Council.

End to End e-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 from the Stoke-on-Trent Education WAN including the effective management of Websense filtering.
- National Education Network standards and specifications.

Roles and Responsibilities
The following section outlines the online safety roles and responsibilities of individuals and groups within the school:

Governors:
Governors are responsible for the approval of the Online Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Governors receiving regular information about online safety incidents and monitoring reports. A member of the Governing Body will be appointed to the role of Safeguarding Champion, which will cover e-Safety.

- regular meetings with persons with responsibility for online safety
- monitoring of online safety incident logs
- monitoring of filtering / change control logs
- reporting the Governing Board
-

Principal and Senior Leaders:

- The Principal has a duty of care for ensuring the safety (including online safety) of members

of the school community, though the day-to-day responsibility for online safety will be delegated to the e-Safety Leader.

- The Principal and the Senior Leadership Team will be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff.
- The Principal / Senior Leaders are responsible for ensuring that the e-Safety Leader and other relevant staff receive suitable training to enable them to carry out their online safety roles and to train other colleagues, as relevant.
- The Principal/ Senior Leaders will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal online safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.
- The Senior Leadership Team will receive regular monitoring reports from the e-Safety Leader.

e-Safety Leader

- takes day to day responsibility for online safety issues and has a leading role in establishing and reviewing the school online safety policies / documents
- Ensures that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place.
- provides training and advice for staff
- liaises with the Local Authority
- liaises with school technical staff
- receives reports of online safety incidents and creates a log of incidents to inform future online safety developments
- reports regularly to Senior Leadership Team

Technical staff
The school's technical staff provider (ICTn) will ensure:

- that the school's technical infrastructure is secure and is not open to misuse or malicious attack
- That the school meets required online safety technical requirements and any Local Authority and other relevant body Online Safety Policy / Guidance that may apply.
- that users may only access the networks and devices through a properly enforced password protection policy
- that they keep up to date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant
- that the use of the school network is regularly monitored in order that any misuse / attempted misuse can be reported to the Principal or e-Safety Leader for investigation / action /sanction
- that monitoring software / systems are implemented and updated as agreed in school policies

Teaching and Support Staff
Are responsible for ensuring that:

- they have an up-to-date awareness of online safety matters and of the current school Online Safety Policy and practices

- they have read, understood and signed the Staff Acceptable Use Policy / Agreement (AUP)
- they report any suspected misuse or problem to the Head teacher/e-Safety Leader for investigation / action / sanction
- all digital communications with students / pupils / parents / carers should be on a professional level and only carried out using official school systems
- online safety issues are embedded in all aspects of the curriculum and other activities
- pupils understand and follow the Online Safety Policy and acceptable use policies
- pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- they monitor the use of digital technologies, mobile devices, cameras etc. in lessons and other school activities (where allowed) and implement current policies with regard to these devices.
- in lessons where internet use is pre-planned students / 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
Will be trained in Online Safety issues and be aware of the potential for serious child protection / safeguarding 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

Pupils:

- are responsible for using the school digital technology systems in accordance with the Pupil Acceptable Use Agreement (AUP)
- need to have a good understanding of research skills and the dangers of AI to avoid plagiarism and uphold copyright regulations
- will be expected to know and adhere to the e-safety rules in classes
- 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 policies on the use of mobile devices and digital cameras. They should also know and understand policies on the taking / use of images and on cyber-bullying
- should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the school's Online Safety Policy covers their actions out of school, if related to their membership of the 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 take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website and information about national/local online safety campaigns and literature. Parents and carers will be encouraged to support the school in promoting good online safety practice and to follow guidelines on the appropriate use of:

- digital and video images taken at school events
- access to parents' sections of the website

Writing and reviewing the e-safety policy
The e-Safety Policy is part of the School Development Plan and relates to other policies including those for ICT and Computing, Bullying and for Child Protection.
The school will appoint an e-Safety Coordinator. This may be the Designated Safeguarding Lead as the roles overlap.
Our e-Safety Policy has been written by the school, building on the Stoke-on-Trent e Safety Policy and government guidance. It has been agreed by senior management and approved by governors.
The e-Safety Policy and its implementation will be reviewed annually.

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

The school Internet access will be designed expressly for pupil use and will include filtering appropriate to the age of pupils.

Whilst regulation and technical solutions are very important, their use must be balanced by educating pupils to take a responsible approach. The education of pupils in online safety is therefore an essential part of the school's online safety provision. Children and young people need the help and support of the school to recognise and avoid online safety risks and build their resilience.

Pupils
Online safety provision is mapped coherently and will be a focus in all areas of the curriculum. Staff will reinforce online safety messages across the curriculum. The online safety curriculum has been designed to be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:
A planned online safety curriculum will be provided as part of Computing/PSHE lessons and will be regularly revisited.

Pupils will be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information.

Pupils will be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.

Students / pupils will be supported in building resilience to radicalisation by providing a safe environment for debating controversial issues and helping them to understand how they can influence and participate in decision-making.

Pupils will be helped to understand the need for the pupil Acceptable Use Policies and encouraged to adopt safe and responsible use both within and outside school.

Staff will act as good role models in their use of digital technologies the internet and mobile devices.
In lessons where internet use is pre-planned, it is best practice that students / 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.

Where students / pupils are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit.

It is accepted that from time to time, for good educational reasons, students may need to research topics (e.g. racism, drugs, and discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Technical Staff (or other relevant designated person) can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need.

Parents/carers
Many parents and carers have only a limited understanding of online safety risks and issues, yet they play an essential role in the education of their children and in the monitoring / regulation of the children's on-line behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

The school will therefore seek to provide information and awareness to parents and carers through:

- Curriculum activities
- Face-to-face workshops run by community members
- Letters, newsletters, the school website, blog and social media feeds
- High profile events / campaigns e.g. Safer Internet Day
- Reference to the relevant web sites/ publications

Advice on filtering systems and educational and leisure activities that include responsible use of the internet will be made available to parents.

Managing Internet Access
Virus protection will be updated regularly on all networked computers.
The school will be responsible for ensuring that the school infrastructure / network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented.

E-mail
Pupils may only use approved e-mail accounts on the school system. Pupils must immediately tell a teacher if they receive offensive e-mail. Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.

Staff must use their email account responsibly and professionally at all times. The official school e-mail service may be regarded as safe and secure and is monitored. Users should be aware that e-mail communications are monitored. Staff and pupils should therefore use only the school e-mail service to communicate with others when in school, or on school systems (e.g. by remote access).

Users must immediately report, to the nominated person – in accordance with the school policy, the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.

Any digital communication between staff and students / pupils or parents / carers (email,social media, chat, and blogs) must be professional in tone and content.

Public Web 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.

E-mail addresses will be published carefully, to avoid spam harvesting. The Principal or nominee will take overall editorial responsibility and ensure that content is accurate and appropriate. The website should comply with the school's guidelines for publications, including respect for intellectual property rights and copyright.

Web Publishing pupils' images and work
Images, published to the web, that include pupils will be selected carefully and will not enable individual pupils to be clearly identified. Pupils' full names will not be used anywhere on the website, particularly in association with photographs. Written permission from parents/carers will be obtained before images of pupils are electronically published to the web. Pupil's work can only be published to the website with the permission of the pupil and parents/carers.

Social networking and personal publishing
The school will block/filter access to social networking sites, except those specifically purposed to support educationally approved practice. Newsgroups will be blocked unless a specific use is approved.

School staff and governors should ensure that:

- First name only reference should be made in social media to pupils, parents / carers or given names for school staff
- No personal information should be disclosed on social networks or in any online space.
- They do not engage in online discussion on personal matters relating to members of the school community
- Personal opinions should not be attributed to the school or local authority
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information

2.3.6 Managing filtering
The school will work with Stoke-on-Trent City Council, Becta and the WAN Managed Service Provider to ensure systems to protect pupils are reviewed and improved. As a school, we are aware that e-Safety does not stand still, and that new threats online can present themselves rapidly. As a result, all staff need to monitor local and national government guidance regularly to ensure that any new issues are made aware to staff and pupils as appropriate.

If staff or pupils discover an unsuitable site, the URL must be reported to the school filtering manager (nominated contact), the e Safety Coordinator or the WAN Managed Service Provider helpdesk.

2.3.7 Managing remote teaching/video-conferencing

Full IP videoconferencing will use the national educational or the schools' broadband network to ensure quality of service and security. All videoconferencing equipment in the classroom must be switched off when not in use and not set to auto answer.

Equipment connected to the educational broadband network will use the national E.164 numbering system and display their H.323 ID name.

External IP addresses will not be made available to other sites.

Videoconferencing contact information will not be put on the school Website.

School videoconferencing equipment will not be taken off school premises without permission, since use over a non-educational network (e.g. the internet) cannot be monitored or controlled.

Users

Pupils will ask permission from the supervising teacher before making or answering a video conference call.

Video conferencing will be supervised appropriately for the pupils' age.

Parents/Carers will agree for their children to take part in videoconferences, probably in the annual return.

Responsibility for the use of the videoconferencing equipment outside school time will be established with care.

Only key administrators will be given access to the videoconferencing system, web or other remote control page available on larger systems.

Unique log on and password details for the educational videoconferencing services will only be issued to members of staff and kept secure.

Content

When recording a videoconference lesson, written permission will be sought by all sites and participants. The reason for the recording is given and the recording of videoconference is clear to all parties at the start of the conference. Recorded material will be stored securely. If third-party materials are to be included, recordings will be checked that they are acceptable to avoid infringing the third party intellectual property rights. Dialogue will be established with other conference participants before taking part in a videoconference. If it is a non school site it is checked that they are delivering material that is appropriate for the class.

Managing emerging technologies

Mobile phones will not be used during lessons or formal school time, unless specifically allowed to support learning as identified by the teacher. Pupils are not allowed to use mobile phones in school. Those children needing to bring a mobile phone into school will be required to complete a parental permission form. Pupil phones will be kept safe in the school office during the school day and then collected from the office at the end of the school day.

The sending of abusive or inappropriate text messages is forbidden.

Protecting personal data

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.

Policy Decisions

Authorising Internet access

The school will maintain a current record of all staff and pupils who are granted access to the school's electronic communications, which includes internet access. The record will be kept up-to-date, for instance a member of staff may leave or a pupil's access be withdrawn.

All staff must read and sign the school AUP before using any school ICT resource.

At EYFS/Key Stage 1 access to the Internet will be by adult demonstration or by directly supervised access to specific, approved on-line materials.

Parents/Carers will be asked to sign and return Acceptable Usage Policies and consent forms to authorise internet access for pupils. This information is contained within the Information sent out to all parents at the start of the children's time at St Peter's Catholic Academy.

Sanctions for inappropriate use will be enforced. These may include notifying parents and/or prohibiting a user from accessing the internet.

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 Stoke-on-Trent City Council can accept liability for the material accessed, or any consequences of Internet access.

The school will audit ICT provision to establish if the e-safety policy is adequate and that the implementation of the e-safety policy is appropriate.
The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990.
Methods to identify, assess and minimise risks will be reviewed regularly.

Handling e-safety complaints
Complaints of Internet misuse will be dealt with by a senior member of staff.
Any complaint about staff misuse must be referred to the Principal.

- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.
- Pupils and parents/carers will be informed of the complaints procedure.
- Parents/Carers and pupils will need to work in partnership with staff to resolve issues.

Cyberbullying – Understanding and addressing the issues
The school will take all reasonable precautions to prevent cyber bullying whilst pupils are in its care. However, due to the global and connected nature of new technologies, it is not possible to guarantee that inappropriate use via a school device (computer or tablet device) will not occur. The school cannot accept liability for inappropriate use, or any consequences resulting outside of school.

The school will proactively engage with pupils as felt appropriate in preventing cyber bullying by:

- Understanding and talking about cyber bullying – the inappropriate use of e-mails, text messages or social networking apps.
- Keeping existing policies and practices up to date with new technologies.
- Ensuring easy and comfortable procedures for reporting (including CEOP and Whisper methods of reporting incidents)
- Promoting the positive use of technology
- Evaluating the impact of prevention activities.

Records of e-Safety incidents such as cyber bullying will be kept and will be used to help to monitor the effectiveness of the school's prevention activities

How will cyberbullying reports/issues be handled?
Complaints of cyberbullying will be dealt with by a senior member of staff. Any complaint about staff misuse must be referred to the Principal.

Evidence of offending messages, pictures or online conversations will be kept, in order to demonstrate to others what is happening. It can be used by the school, internet service provider, mobile phone company, or the police, to investigate the cyberbullying.

Pupils and parents/carers will be informed of the complaints procedure.
Parents/Carers and pupils will need to work in partnership with staff to resolve issues.

Communications Policy
Introducing the e-safety policy to pupils
E-safety rules will be posted in all networked rooms and discussed with pupils at the start of each year and as the need arises. Pupils will be informed that network and Internet use will be monitored.

Instruction in responsible and safe use should precede Internet access. E-safety will be delivered throughout the year. e-Safety teaching will be included in the PSHE or Computing programmes covering both school and home use.

Staff and the E-Safety policy

It is essential that all staff read and understand the e-Safety Policy. The application and importance of the policy will be explained.

All staff will be informed that all computer and Internet use will be monitored. Discretion and professional conduct is essential.
Staff training in safe and responsible Internet use and on the school e Safety Policy will be provided as required.
Staff that manage filtering systems or monitor ICT use will be supervised by senior management and have clear procedures for reporting issues.

Enlisting parents/carers support
Parents/Carers' attention will be drawn to the School e-Safety Policy in newsletters and on the school website.
Parents/Carers are welcome to bring any issues to staff to deal with.
Parents/Carers will be kept informed about e-safety teaching.

Reviewed January 2026p