Online Safety Policy

Our Vision
"Many Hearts, One Accord"
"Do whatever He tells you"

We are the many hearts that follow Jesus, the one accord.
"Through the strength of God's love and the power of prayer
we are guided to do whatever He tells us. Many hearts,
one accord, growing and learning together for life to build the kingdom of God."
(School Mission Statement)

Approved by: Local Academy Committee	**Date:** November 2022
Last reviewed on:	
Next review due by:	November 2023

Online Safety Policy

Online 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.

The school's online safety policy operates in conjunction with other policies including those for Anti Bullying, Curriculum, Data Protection and Security.

1.1 End to End Online Safety

Online 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 online 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.

School Online Safety Policy

- # 2.1 Teaching and Learning

- **2.1.0 The Importance of new technologies and Internet use.**
  - 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.

2.1.1 The Use of the Internet to enhance teaching and learning

- At St Mary's and Our Lady of Grace Catholic Academies, Internet access is designed expressly for pupil use and includes filtering appropriate to the age of pupils.
- Pupils are taught about what Internet use is acceptable and what is not and are given clear objectives for Internet use.
- Internet access is planned to enrich and extend learning activities. All pupils have equal access to internet content.
- Pupils are guided in online activities that will support the learning outcomes planned for the pupils' age and maturity.
- Pupils will be educated in the effective use of the Internet in research, including the skills of effective knowledge location, retrieval and evaluation.

2.2.1 Enabling pupils to evaluate Internet content

Members of staff at St Mary's and Our Lady of Grace Catholic Academies ensure that the copying and subsequent use of Internet derived materials by staff and pupils complies with copyright law.

- Pupils are be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy. They will be aware of the need to evaluate information and that copying and pasting large amounts of text is unacceptable without identifying the source.

2.2.2 Ensuring Pupils Stay Safe Online

Curriculum planning will include age appropriate opportunities to discuss, role play and learn about the benefits and risks offered by new technologies, such as e-mail, mobile phones and social networking sites.

- Online safety delivery will be mapped across the curriculum to ensure full coverage.

2.3 Managing Internet Access

2.3.1 Information system security

- Virus protection is updated regularly on all networked computers through LA and ETS support.
- School ICT systems capacity and security will be reviewed regularly.
- Security strategies will be discussed through the schools' technical support and through attendance at LA updates. Representation by the school is made at LA e safety updates.

2.3.2 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.
- The forwarding of chain letters is disallowed and the potential harm that can be caused will be included within e-safety learning.

2.3.3 Public Web published content and the school web site

- The contact details on the website is the school address, e-mail and telephone number. Staff or pupils' personal information will not be published. Staff school E-mail addresses may be published is agreed by both parties.
- E-mail addresses will be published carefully, to avoid spam harvesting.
- The Headteacher, business manager 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.

2.3.4 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 or carers will be obtained before images of pupils are electronically published to the web.

Pupils' work can only be published to the website with the permission of the pupil and parents.

2.3.5 Social Networking and Personal Publishing

The City Council will block access to social networking sites, except those specifically purposed to support educationally approved practice.

Newsgroups will be blocked unless a specific use is approved.

Staff and pupils will be advised never to give out personal details of any kind which may identify them or their location.

- Pupils and parents will be advised that the use of social network spaces, outside school based controlled systems (i.e. SCORE/ Learning Platform), is inappropriate for primary aged pupils, unless strictly supervised.
- Staff and pupils should be advised not to publish specific and detailed private thoughts on social networking sites. The school or anything related to the school should never be mentioned on social networking sites. The school has a clear protocol for this and breach of this procedure could result in disciplinary action being taken.

2.3.6 Managing Filtering

- The school will work with Stoke-on-Trent City Council, Staffordshire County Council, Becta and the WAN Managed Service Provider to ensure systems to protect pupils are reviewed and improved.
- If staff or pupils discover an unsuitable site, the URL must be reported to the school filtering manager (nominated contact), the Online Safety Coordinator or the WAN Managed Service Provider helpdesk.
- Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

.

2.3.7 Managing Remote Teaching/Video-Conferencing

The equipment and network

Full IP videoconferencing (if used) 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 videoconference call.

Videoconferencing will be supervised appropriately for the pupils' age.

Parents and guardians 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.

2.3.8 Managing Emerging Technologies

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out and protocols established before use in school is allowed.
- Mobile phones will not be used during lessons or formal school time, unless specifically allowed to support learning as identified by the teacher. The sending of abusive or inappropriate text messages is forbidden.

2.3.9 Protecting Personal Data

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

2.4 Policy Decisions

2.4.1 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 read and sign the 'Staff Information Systems Code of Conduct' before using any school ICT resource.
- Parents will be asked to sign and return a consent form.
- Sanctions for inappropriate use will be drawn up and shared with staff and pupils.

2.4.2 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 online safety policy is adequate and that the implementation of the online 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.

2.4.3 Handling Online 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 Headteacher.
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.
- Pupils and parents will be informed of the complaints procedure.

Parents and pupils will need to work in partnership with staff to resolve issues.

- Sanctions within the school discipline policy will include:
    - interview/counselling by the head teacher/ senior manager
    - informing parents or carers;
    - removal or restriction of Internet or computer access for a period.
- Discussions will be held with the Police Youth Crime Reduction Officer to establish procedures for handling potentially illegal issues.

2.4.4 Community use of the Internet

- The school will liaise with local organisations to establish a common approach to online safety.

2.4.5 Online Bullying – Understanding and addressing the issues

- While online bullying is likely to be low level in primary schools, the age of pupils making proficient use of technology is ever decreasing. Therefore, the opportunities for pupils to bully or be bullied via technology, such as e-mail, texts or MSN, are becoming more frequent.
- As such, teaching pupils about appropriate behaviours when using technology provides a vital grounding for future use. Whilst not wanting to provoke unrecognised opportunities in pupils, consideration must be given to suitable teaching and procedures to address any issues of online bullying.
- As felt appropriate for the age and use of technology by the pupils:
    - The school's anti-bullying policy and/or school behaviour policy will address online bullying. Online bullying will also be addressed in Computing, PHSE and other relevant lessons and is brought to life through activities. As with other whole-school policies, all staff and young people will be included and empowered to take part in the process.
    - Pupils, parents, staff and governors will all be made aware of the consequences of online bullying. Young people and their parents will be made aware of pupils' rights and responsibilities in their use of new technologies, and what the sanctions are for misuse.
    - Parents will be provided with an opportunity to find out more about online bullying through: session for parents, guidance, Know It All parents' CD, etc.

2.4.6 Cyber-Bullying - How will risks be assessed?

- The school will take all reasonable precautions to ensure against online 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 computer will not occur. Neither the school, nor Stoke-on-Trent City Council, can accept liability for inappropriate use, or any consequences resulting outside of school.
- The school will proactively engage with KS2 pupils in preventing online bullying by:

- understanding and talking about online bullying, e.g. inappropriate use of e-mail, text messages;
- keeping existing policies and practices up-to-date with new technologies;
- ensuring easy and comfortable procedures for reporting;
- promoting the positive use of technology;
- evaluating the impact of prevention activities.

- Records of any incidents of online bullying will be kept and will be used to help to monitor the effectiveness of the school's prevention activities.
- 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.

2.4.7 The Handling of Cyber-Bullying Reports/Issues

Complaints of online bullying will be dealt with by a senior member of staff.
Any complaint about staff misuse must be referred to the headteacher.
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 online bullying.

- Pupils and parents will be informed of the complaints procedure.
- Parents and pupils will need to work in partnership with staff to resolve issues.
- Sanctions within the school discipline policy include:
  - interview/counselling by the class teacher/ headteacher;
  - informing parents or carers;
  - removal of Internet/computer access for a period or banning of mobile phone in school.

2.5 Communications Policy

2.5.1 Introducing the Online Safety Policy to Pupils

- Online 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.
- An Online Safety training programme will be introduced to raise the awareness and importance of safe and responsible internet use.
- Instruction in responsible and safe use should precede Internet access.
- An Online Safety module will be included in the PSHE, Citizenship or Computing programmes covering both school and home use.

2.5.2 Staff and the Online Safety Policy

- All staff will be given the School Online Safety Policy and its application and importance 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 Online Safety Policy will be provided as required.

2.5.3 Enlisting Parents' Support

- Parents' attention is drawn to the School Online Safety Policy in newsletters, the school brochure, on the school website and through parents' sessions.
- Internet issues are be handled sensitively, and parents advised accordingly.
- A partnership approach with parents is encouraged at St Mary's and Our Lady of Grace Catholic Academies; this includes parent evenings with demonstrations and suggestions for safe home Internet use.
- Advice on filtering systems and educational and leisure activities that include responsible use of the Internet is made available to parents at regular intervals.
- Online safety updates are communicated to parents on the school websites, as well as via our monthly messengers, using the NOS (National Online Safety) online toolkit.

3.1 Remote Learning

3.1.1 Rationale

Remote Learning is an essential part of raising pupil achievement at all key stages. Remote learning is also essential in the current circumstances in order that learning can continue at home where it is not possible in school. Remote learning is in place to ensure there are no barriers to ensuring pupils can continue working with the curriculum. The aim is to ensure that all children can continue to follow the curriculum if they have authorised absence from school.

3.1.2 Protocols (PEC & ROLLS)

Staff will ensure the following protocols are checked before (PEC), during and after (ROLLS) remote learning takes place:

PEC

P: Proof-read and double check the document you have uploaded is the correct one. It sounds silly but drag and drop can easily mean you have uploaded a document that you did not mean to and can cause unnecessary delays and complications.

E: Ensure your environment for an online lesson is appropriate. Guidance from both the TES and safeguardinginschools.co.uk suggests using a blank background and where possible, not using a bedroom and turning your webcam on to be sure that nothing inappropriate or distracting can be seen. A suitable background would be a blank wall for instance. You should also let the people in your household know you are going online – this helps to minimise a partner or flatmate walking in to shot. There is of course also the option of just turning your camera off if you are more comfortable with this.

C: Check your clothing before an online lesson. You should ensure you are dressed in line with the Collegiate Dress Code. You must ensure you check for things such as inappropriate slogans and that it appropriately covers at the angle of the webcam. Sit where you would sit with the webcam on and look to check you are happy with how you appear on the screen and with the clothing you are wearing.

ROLLS
R: Record as soon as you begin the lesson and be the first one to exit the lesson. Never leave yourself unrecorded or in a one to one conversation online with a pupil.

O: Off! Insist on all microphones off before you begin and stop if this rule is broken. Pupils can comment using the 'chat' function. Should a pupil behave inappropriately, immediately end the lesson and contact a line manager. Also put down in writing, immediately after, what happened in as much detail as you can remember.

L: Length! Check your lesson or task is not too long. Frequently, pupils are hindering parents / siblings' use of the internet by tuning in or doing the work. 30-45 minutes is enough for an online lesson or a task.

L: Language! Keep language professional during your task or online lesson and minimise the chances of another member of the household to be overheard using inappropriate language. If you have a set of headphones which include a microphone, such as those that come with iPhones, using these helps minimize outside noise. Don't share personal information within the lesson with your pupils.

S: Save. Check that the recording is being posted on Teams. This serves two important uses: Firstly, for pupils who cannot access your live lesson – possibly due to family commitments or being ill themselves, they can ensure they do not miss out. Secondly, if an accusation was to be made against you in the future, this recording is evidence that you have behaved appropriately.

4.1 Writing and Reviewing the Online Safety Policy

The Online Safety Policy is part of the School Development Plan and relates to other policies including those for Computing, Bullying and for Child Protection.

- The school has appointed an Online Safety Coordinator. This is also the Designated Child Protection Coordinator as the roles overlap.
- Our Online Safety Policy has been written by the school, building on the Stoke-on-Trent Online Safety Policy and government guidance. It has been agreed by senior management, all staff and approved by governors.

This policy was agreed by staff: November 2022

This policy was approved by School Committee on: November 2022

This policy will be reviewed by the School Committee on

Signed_____Chair of School Committee

Online Safety Audit – Primary

This audit has enabled the SMT to assess whether the online safety basics are in place to support a range of activities that might include those detailed within Appendix 1.

Has the school an Online Safety Policy that complies with C&YP guidance?	**Y**/N
Date of latest update:	
The Policy was agreed by governors on:	
The Policy is available for staff at: School Website	
And for parents at: the office	
The Designated Child Protection Coordinator is: S Rathbone	
The Online Safety Coordinator is: M Zoumides	
Has online safety training been provided for staff?	Y
Has online safety training been coherently planned and delivered for pupils?	Y
Do all staff sign an ICT Code of Conduct on appointment?	Y
Do parents sign and return an agreement that their child will comply with the school Online Safety Rules?	Y
Have school Online Safety Rules been set with pupils?	Y
Are these Rules displayed in all rooms with computers?	Y
Internet access is provided by an approved educational Internet service provider and complies with DCSF requirements for safe and secure access (e.g. Stoke-on-Trent Educational WAN).	Y
Is personal data collected, stored and used according to the principles of the Data Protection Act?	Y
Do all school computers have e-safety text monitoring software (Forensic) installed?	Y
Has the school filtering policy been approved by SMT? (N/A unless school has taken over responsibility)	Y
If the school has taken responsibility for its own webfiltering, have appropriate members of staff attended training on the filtering system and are appropriate procedures in place?	NA
Is an ICT security audit advisable (possibly using external expertise) to ensure online safe practice technically and educationally?	N

Appendix 1: Internet use - Possible teaching and learning activities

Activities	Key Online Safety Issues	Relevant Websites
Creating web directories to provide easy access to suitable websites.	Parental consent should be sought. Pupils should be supervised. Pupils should be directed to specific, approved on-line materials.	Web directories e.g. Networked favourites Ikeepbookmarks.com SCORE minisites
Using search engines to access information from a range of websites.	Parental consent should be sought. Pupils should be supervised. Pupils should be taught what internet use is acceptable and what to do if they access material they are uncomfortable with.	Web quests e.g. - Ask Jeeves for kids - Yahooligans - CBBC Search - Kidsclick
Exchanging information with other pupils and asking questions of experts via e-mail.	Pupils should only use approved e-mail accounts. Pupils should never give out personal information. Consider using systems that provide online moderation e.g. SuperClubs.	SCORE sgfl accounts School Net Global E-mail a children's author E-mail Museums and Galleries
Publishing pupils' work on school and other websites for feedback.	Pupil and parental consent should be sought prior to publication. Pupils' full names and other personal information should be omitted. Pupils should be encouraged to report any inappropriate comments.	SCORE Showcase Making the News Podcasts
Publishing images including photographs of pupils.	Parental consent for publication of photographs should be sought. Photographs should not enable individual pupils to be identified. File names should not refer to the pupil by name.	Making the News SuperClubs Learninggrids Museum sites, etc. Digital Storytelling BBC – Primary Art
Communicating ideas within blogs, chat rooms or online forums.	Only blogs/chat rooms dedicated to educational use and that are moderated should be used. Access to other social networking sites should be blocked. Pupils should never give out personal information.	SCORE Blogs SuperClubs Skype FlashMeeting VLE
Audio and video conferencing to gather information and share pupils' work.	Pupils should be supervised. Only sites that are secure and need to be accessed using an e-mail address or protected password should be used.	Skype FlashMeeting National Archives "On-Line" Global Leap National History Museum Imperial War Museum