St Wilfrid's Catholic Academy

"Love One Another As I Have Loved You"

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.

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

The C&YP Core e-Safety Policy
St Wilfrid's e-safety policy was based on the core e-Safety policy which has been approved by Stoke-on-Trent's Children and Young People's Services (C&YP). The C&YP policy considers that all the elements below are mandatory in order to protect users, the school the Newman catholic Collegiate 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.

School e-Safety policy
The bullets below are the essential guidelines St Wilfrid's have chosen to take from the C&YP core e Safety Policy.

These elements enable our school to demonstrate that it has an e-Safety Policy which is compliant with the C&YP approved policy.

2.1 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, Bullying and Safeguarding.

The school appointed e-Safety Coordinator is Mr Tooth.

- 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 our Local Academy Committee and our Directors.
- The e-Safety Policy and its implementation will be reviewed annually.

2.2 Teaching and learning

2.2.1 Why are new technologies and Internet use important?

- 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.

2.2.2 Internet use will enhance learning.

The school Internet access is designed expressly for pupil use and will include filtering appropriate to the age of pupils. Pupils will be taught what Internet use is acceptable and what is not and will be given clear objectives for Internet use. Pupils will be educated in the effective use of the Internet in research, including the skills of effective knowledge location, retrieval and evaluation.

2.2.3 Pupils will be taught how to evaluate Internet content.

The school will ensure that the copying and subsequent use of Internet derived materials by staff and pupils complies with copyright law. Pupils should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

2.2.4 Pupils will be taught how to stay e-Safe.

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.

- e-Safety delivery will be mapped across the curriculum to ensure full coverage.
- e-Safety delivery will include the safe use of mobile phones.
- e-Safety delivery will also include emerging and developing technologies such as gaming.

2.3 Managing Internet Access

2.3.1 Information system security

Virus protection will be updated regularly on all networked computers.
School ICT systems capacity and security will be reviewed regularly.

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.

2.3.3 Public Web published content and the school web site
The contact details on the website are 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 Headteacher, Mr Barlow, 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/carers will be obtained before images of pupils are electronically published to the web. This is done at the point of sign up in school and parents have the responsibility to let the school know if their decion on photography changes. Pupil's work will only be published to the website with the permission of the pupil and parents/carers.

2.3.5 Social networking and personal publishing
St Wilfrid's will block access to social networking sites and Newsgroups, except those specifically purposed to support educationally approved practice.
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/carers will be advised that the use of social network spaces, outside school based controlled systems, is inappropriate for primary aged pupils. Parents will be regularly signposted to age limits for popular social networking sites and a section on our website will guide parents to safe internet use for pupils.
Staff and pupils are advised not to publish specific and detailed private thoughts on social networking sites. Staff are not permitted to include pupils on any list of "friends" on any social media platform.

2.3.6 Schools use of Class Dojo.
We use Class Dojo as part of our behaviour management system. This is documented in our Behaviour Policy. Parents are kept informed of their child's progress throughout the day by the Class Dojo App where parents are given an invite code to view their child's Class Dojo avatar on line. Class Dojo is used in line with policy set out above (2.3.3, 2.3.4, 2.3.5).

The system also allows for direct and private messages to be sent to or from the teacher. Where message content is deemed to be inappropriate by either home or school this will be raised directly with the Class Dojo Moderator, Mr Barlow. Any issues will be discussed and resolved through refining protocols.

Class Dojo also gives teachers the opportunity to post information to a Class Story or to a School Story. Here, members of Class Dojo (parents) can "like" posts or leave comments about them. Where posts or comments are deemed to be inappropriate this can be raised with the Class Dojo Moderator, Mr Barlow. Any posts that are deemed unsuitable will be removed from the Class or School Story.

The Class Dojo Moderator, Mr Barlow, will make all decisions to remove posts and inform the Chair of the Local Academy Committee, Mr Hassall, where this action has been taken. Where posts are removed this will be followed up by a direct conversation with the person responsible for the content deemed inappropriate.

2.3.7 Managing filtering

The school will work with our LAN 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 (Mr Barlow), the e-Safety Coordinator (Mr Tooth) or the LAN Managed Service Provider (Alex Lynch). The site will then be blocked on our system.

Mr Barlow will carry out regular review of how the internet is used on both pupil and staff machines. Any breaches will be dealt with in accordance with our discipline policy and alongside our Social Media Policy. A record of findings will be kept securely so that the school community can be assured of our commitment to keeping pupils safe online.

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.

2.3.9.1.Mobile phones

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.

As a general rule mobile phones are not allowed in school. As pupils grow in their independence particularly in Year 5 and Year 6, there may be times that mobile phones are allowed in school, for example if the child has written parental permission to walk to and/or from school. In this instance pupils will take their phone directly to the school office on arrival and collect it at the end of the school day. Pupils are told that they must not use the phone whilst on the school site, instead reporting any issues to staff.

Pupil i-Pads will use the school filtered network so that our systems will block inappropriate content.

School owned laptops will be monitored for inappropriate content, using key search software, both inside and outside school. This will maintain safety for all involved.

Monitoring activities carried out by Senior Leaders will be documented.

2.3.8 Protecting personal data
Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 until the 25th May 2018 and after this point in line with General Data Protection Regulation.

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, once the user agreement has been signed, 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. This will be maintained by Mr Tooth, our ICT Lead.

All staff must read and sign the 'Staff Information Systems Code of Conduct' before using any school ICT resource.

At 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 a consent form. Sanctions for inappropriate use will be drawn up based on each individual case and shared with staff and pupils and will be in line with our Behaviour Policy.

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 the Newman Catholic Collegiate can accept liability for the material accessed, or any consequences of Internet access.

St Wilfrid's 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. In the event of this happening we will follow procedures set out in our Discipline Policy (staff) or Behaviour Policy (pupils).

Methods to identify, assess and minimise risks will be reviewed regularly.

2.4.3 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 Headteacher (Mr Barlow).
- 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.
- Sanctions within the school discipline policy will include:
    - interview/counselling by the head of key stage;
    - informing parents or carers;
    - Removal or restriction of Internet or computer access for a period.

2.4.4 Community use of the Internet
St Wilfrid's does not currently engage in any community use of internet.

2.4.5 Cyberbullying – Understanding and addressing the issues
While cyberbullying 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 social media, 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 previously unrecognised opportunities in pupils, consideration must be given to suitable teaching and procedures to address any issues of cyberbullying.

The school's Anti-Bullying Policy and School Behaviour Policy addresses cyber bullying. Cyberbullying is also addressed in ICT, 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 are exposed to regular high quality whole school assemblies to discuss such issues.

Pupils, parents/carers, staff and Local Academy Committee members will all be made aware of the consequences of cyberbullying. Young people and their parents/carers will be made aware of pupils' rights and responsibilities in their use of new technologies, and what the sanctions are for misuse.

Parents/Carers will be provided with an opportunity to find out more about cyberbullying through e-safety sessions planned for parents and offered at 2.00pm and 6.30pm on the same day with the same content. Parents and carers will also be regularly signposted to relevant information through the use of our website, text system and Class Dojo.

2.4.6 Cyberbullying – How will risks be assessed?
St Wilfrid's will take all reasonable precautions to ensure against cyberbullying 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 the Newman Catholic Collegiate, can accept liability for inappropriate use, or any consequences resulting outside of school.

The school will proactively engage with KS 1 and 2 pupils in preventing cyberbullying by:
- understanding and talking about cyberbullying, 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 to adults or e-Safety Officers
- promoting the positive use of technology;
- evaluating the impact of prevention activities.

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

2.4.6.1 e-Safety Officers

St Wilfrid's Catholic Academy operates an additional route for reporting issues that pupils may face through the promotion of e-Safety Officer Officer roles that are filled solely by pupils. At the beginning of each academic year pupils in Y2-Y6 will express an interest in becoming an e-Safety Officer, via a letter to the Headteacher. Those pupils subsequently chosen will receive a special e-Safety Officer badge, bespoke training, termly meetings with the Headteacher and their role promoted in assembly. The e-Safety officers will report any issues that are brought to them by pupils and are trained to pass on information. All other pupils know that if they share information with an e-Safety Officer that it will be shared with a member of staff.

2.4.7 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 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 cyber bullying.
- 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.

2.5 Communications Policy

2.5.1 Introducing the e-Safety policy to pupils

e-Safety rules will be posted in all classrooms 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 e-Safety training programme has been included in each school year to raise the awareness and importance of safe and responsible internet use and the safe use of mobile technology.
- Instruction in responsible and safe use should precede Internet access.
- An e-Safety module will be included in the PSHE, Citizenship and ICT programmes covering both school and home use.

2.5.2 Staff and the e-Safety policy

All staff will be given the School e-Safety Policy and its application and importance explained.
All staff will be informed that all computer and Internet use will be monitored. 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.

2.5.3 Enlisting parents/carers support
Parents/Carers' attention will be drawn to the School e-Safety Policy in newsletters, on the school website, through the e-safety team and through parents/carers awareness sessions held regularly.

- Parents/Carers views and ideas will be canvassed by questionnaires.
- Parents/Carers are welcome to bring any issues to staff to deal with.
- Parents/Carers will be kept informed about e-safety teaching as is takes place each term.

Reviewed January 2018

Adopted by Governors June 2018
Next review date September 2020