E-Safety and Sexting Policy

St John Chrysotom's Federation

Autumn 2017

St. John Chrysostom's Federation E-safety and Sexting Policy

E-safety encompasses Internet technologies and electronic communications such as mobile phones and wireless technology. It highlights the need to educate children and young people about the benefits and risks of using new technology and provides awareness for users to enable them to control their online experiences.

The E-safety and Sexting policy will be reviewed annually. This policy will next be reviewed Autumn 2018.

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 network design and use.
- Safe and secure broadband from One Education including the effective management of content filtering.

Rationale - Why is Internet use important?

The purpose of the Internet use in school is to raise 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 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 of school and will need to learn how to evaluate Internet information and to take care of their own safety and security.

Benefits of using the Internet and how it will enhance learning:

- Access to world-wide educational resources including museums and art galleries.
- Educational and cultural exchanges between pupils and staff.
- Access to experts in many fields for pupils and staff.
- Internet access will be planned to enrich and extend learning activities
- The school Internet access will be designed expressly for pupil use and will include filtering appropriate to the age of pupils.
- Staff will guide pupils in on-line activities that will support learning outcomes planned for the pupil's age and maturity.

Pupils will develop an understanding of the uses, importance and limitations of the internet

- Pupils will be taught how to effectively use the internet for research purposes.
- Pupils will be taught to evaluate information on the internet.
- Pupils will be taught how to report inappropriate web content.
- Pupils will develop a positive attitude to the internet and develop their ICT capability through both independent and collaborative working.
- Pupils will use the internet to enhance their learning experience.
- Pupils have opportunities to engage in independent and collaborative learning using the internet and other digital technologies.

Pupils will use existing technologies safely

- Pupils will be taught about e-safety.

Authorised Internet Access

The school will maintain a current record of all staff and pupils who are granted Internet access. All staff must read and sign the 'Acceptable ICT Use Agreement' before using any school ICT resource. School will also ensure that use of Internet derived materials are shown and how to validate information before accepting its accuracy.
Parents will be informed that pupils will be provided with supervised Internet access and they will be asked to sign and return a consent form for pupil access.

Email

Pupils in KS2 will be taught how to manage e-mail accounts safely.
Pupils may only use the approved accounts on the school system and access to external personal email accounts will be blocked.
Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.
Pupils must tell an adult immediately if they receive offensive email.

Staff are to only access their work emails through the schools internet system. This is in line with the acceptable use policy – See appendix 1.

Social Networking

School blocks access to social networking sites and newsgroups unless specific use is approved. Pupils will be advised never to give out personal details of any kind which may identify them or their location and not to place personal photos on any social network space. Pupils are also advised on security and encouraged to set passwords, deny access to unknown individuals and instructed how to block unwanted communication. Pupils should be encouraged to invite known friends only and deny access to others. The teaching of E-safety is ongoing and embedded in Curriculum where access to the Internet is used to enhance learning.

Published content on the school website and welcoming multimedia (Anomaly etc.)

The contact details on the website should be the school address, email and telephone number. Staff and pupils personal information will not be publish.

Written permission from parents and carers will be obtained before photographs of pupils are published on the website. Photographs that include pupils will be selected carefully ensuring pupils who do not have permission from parents are not published.

Pupils' full names will not be used anywhere on the Web site, including in blogs, forums or wikis, particularly in association with photographs.

Parents should be clearly informed of the school policy on image taking and publishing, both on school and independent electronic repositories. Staff will not keep images of the children on personal devices e.g. memory sticks, or use them for any other use other than in school.
Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998

Managing emerging technologies and Mobiles

Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed

Mobile phones will not be used during lessons or formal school time. The sending of abusive or inappropriate text messages is forbidden. Staff should not share personal telephone numbers with pupils and parents. A school phone will be provided for staff where contact with pupils is required.

Sexting

Someone taking an indecent image of themselves and sending to their friends or boy / girlfriend via a mobile phone or some other form of technology is sometimes referred to as 'Sexting'. Young people need to be aware that they could potentially be distributing illegal child images. We know this can cause enormous distress to children and young people and may place them at risk of sexual grooming and other risks associated with the internet.

'Youth produced sexual imagery' best describes the practice because:
• 'Youth produced' includes young people sharing images that they, or another young person, have created of themselves.
• 'Sexual' is clearer than 'indecent.' A judgement of whether something is 'decent' is both a value judgement and dependent on context.
• 'Imagery' covers both still photos and moving videos (and this is what is meant by reference to imagery throughout the document).

Staff working at St Johns Chrysostom's Federation will ensure that are aware of the risks associated with the use of the internet and how to respond appropriately to a 'Sexting' incident. The learning about youth produced sexual imagery will be taught through a combination of PSHE, as well as through the school's computing programme (Switched on computing – Rising Stars).

"Teaching should also reflect the principles articulated in 'Key principles of effective prevention education' - produced by the PSHE Association on behalf of NCA-CEOP.22 Given the potential sensitivity of these lessons it is essential that this issue is taught within an emotionally safe classroom climate where clear ground rules have been negotiated and established and where boundaries around teacher confidentiality have been clarified. If during any lesson teachers suspect any child or young person is vulnerable or at risk the school's safeguarding protocols should always be followed." – UK Council for child Internet Safety Jan 2017 (Sexting in Schools and Colleges).

Policy Decisions

Authorising Internet access

- All staff must read and sign the staff 'Acceptable use of ICT' before using any school ICT resource (Appendix 1)
- The school will maintain current record of all staff and pupils who are granted access to school ICT systems
- Parents will be asked to sign and return a consent form (Appendix 2)
- All children must comply with the responsible Internet use statement before being granted Internet access (Appendix 3)
- Any person not directly employed by the school will be asked to sign an 'acceptable use of school ICT resources' form before being allowed to access the internet on the school site.

Assessing risks

The school will take all responsible precautions to prevent access to inappropriate material. However, due to international scale and linked content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither the school nor Wigan MBC can accept liability for material accessed, or any consequences of internet access.
The school will audit ICT use to establish if the E-safety is adequate and that the implementation of the E-safety policy is appropriate and effective.

Handling E-safety complaints

Complaints of internet misuse will be dealt with by a senior member of staff. Any compliant about staff misuse must be referred to the Head teacher. Complaints of a child protection nature must be referred to the Senior Designated Professional for Safeguarding and dealt with in accordance with the school child protection procedures.
Both pupils and parents will be informed of the complaints procedure and informed of the consequences for pupils misusing the internet.

Communications

Introducing the E-safety policy to the pupils

- Appropriate elements of the E-safety policy will be shared with pupils.
- E-safety rules will be posted in the Discovery room
- Pupils will be informed that network and internet use will be monitored
- Curriculum opportunities to gain awareness of E-safety issues and how best to deal with them will be provided for pupils.

Staff and the E-safety policy

- All staff will be given the school E-safety policy and its importance explained.
- Staff should be aware that internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.
- Staff who manage filtering systems or monitor ICT use will be supervised be senior management and will have clear procedures for reporting issues.

Enlisting parents' support

- Parents and carers attention will be drawn to the schools E-safety policy in newsletters, the school brochure and on the school website.
- Parents and carers will from time to time to provided with additional information on E-safety.
- The school will ask all new parents to sign the parent/ pupil agreement when they register their child with the school.
- Parents and carers will be reminded that they must not publish any images or comments of performances and other community events on social networking sites.

This policy should be read in conjunction with the St John Chrysostom's Federation Safeguarding Policy.

Appendix 1

Staff Acceptable use of ICT

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 E-safety and Sexting 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 E-safety Coordinator or the Designated Child Protection Coordinator.

· I will ensure that any electronic communications with pupils are compatible with my professional role.

· I will promote E-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: …….. Date: ……

Appendix 2

PUPIL GUIDELINES FOR SAFE INTERNET USE

I will only use the Internet when there is a teacher present.
I will only use my own usernames and passwords to log on to the system
I will not access other people's files.
I will only email people I know, or my teacher has approved and ensure that the messages that I send will be polite and responsible.
I will not give personal details (like my home address, telephone or mobile number), or the personal details of any other person to anyone, or arrange to meet someone unless my parent/carer or teacher has given me permission.
I will avoid any acts of vandalism. This includes, but is not limited to, uploading or creating computer viruses and mischievously deleting or altering data from its place of storage.
Use the Internet for research and school purposes only.
I will not bring in memory sticks or CD Roms from home to use in school unless I have been given permission by my class teacher.
I understand that the school may check my computer files/Emails/KLP and may monitor the Internet sites that I visit.
I understand that if I don't follow these rules, my access to the school computer system may be suspended, and my parents/carers will be informed.

Pupil's Name		**Class Teacher**	
As a school user of the Internet, I agree to follow the school rules on its' use. I will use the network in a responsible way and observe all the restrictions explained to me by my school.			
Pupil Name (print)			
Pupil Signature		**Date**	