St. Wilfrid's Church of England Primary Academy

Online Safety Policy

June 2017

Our Christian Values

As a Voluntary Aided Church of England Primary Academy, we have eight Christian Values, underpinned by love at the heart of everything we do.

Our Christian Values are:

Fair, Kind, Joy, Courage, Forgive, Hope, Peace and Trust
Love

Introduction

The Online Safety Policy is part of the School Development Plan and relates to other policies including those for safeguarding, computing, anti-bullying, and data protection.

Our Online Safety Policy has been written by the school, building on the Wigan Online Safety Policy and government guidance. It has been agreed by senior management and approved by governors.

Teaching and learning

Why the Internet and digital communications are important

- The Internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide pupils with quality safe 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.

- We support our pupils' use of the internet and seek to underpin their knowledge of safe use and protection.

- We provide our pupils with an awareness of how to stay safe online both in the school environment and beyond, and encourage them to be digitally resilient.

- We believe that children should adhere to the certification given to games, DVD's etc.

Internet use will enhance and extend learning

- Staff will be made aware of and pupils will be educated in the safe use of the internet.

- To ensure staff have regular updates regarding new technologies/ICT resources and in particular receive regular updates through staff training on current/new Online Safety issues

- Clear boundaries will be set and discussed with staff and pupils for the appropriate use of the internet and digital communications (acceptable use policy).

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

- Impero Software will be used to monitor use of the internet and to highlight violations by all users.

- Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.

- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.

Pupils will be taught how to evaluate Internet content

 The school will ensure that the use of Internet derived materials by staff and pupils complies with copyright law.

 Pupils will be taught the importance of cross-checking information before accepting its accuracy.

 Pupils will be taught how to report unpleasant Internet content e.g. Using the CEOP Report Abuse icon, speaking to an adult.

Cyber Bullying

Cyber Bullying is action repeated over time taken by one or more children with the deliberate intention of hurting them emotionally via text messages or the internet. Awareness will be raised of these issues and how the children can address them during our Online Safety units of work and regular themed days.

Internet Access

Information system security

- ICT systems security will be reviewed regularly including Impero software which monitors use by all users.
- Virus protection will be updated regularly (Sophos)
- Security strategies will be discussed with the internet provider (Virtue Technologies).
- E-mail and other forms of social media
- Pupils may only use approved e-mail accounts on the school system.
- Pupils must be made aware of how they can report abuse and who they can report abuse to.
- Pupils must immediately tell a teacher if they receive offensive e-mail or messages in school.
- In online communication, pupils must not reveal their personal details or those of others, or arrange to meet anyone without specific permission.
- Incoming e-mail and messages should be treated as suspicious and attachments not opened unless the author is known. Filters are in place via Virtue Technologies.
- The school considers how e-mail and messages from pupils to external bodies is presented and controlled.
- The forwarding of chain letters and emails is not permitted.

Published content and the school web site

- Staff or pupil personal contact information will not be published. The contact details given online are for the school office.
- The Headteacher will take overall editorial responsibility and ensure that content is accurate and appropriate.

Publishing pupil's images and work

- Photographs that include pupils will be selected carefully so that individual pupils cannot be identified or their image misused. The school will consider using group photographs rather than full-face photos of individual children where appropriate.

- Pupil's full names will not be used anywhere on the school Website or other on-line space, particularly in association with photographs.

- Written permission from parents or carers will be obtained as part of the general permission slip, before photographs of pupils are published on the school Website or other on-line space.

- Parents should be clearly informed of the school policy on image taking and publishing, both on school and independent electronic repositories and permissions for photographs sought from parents/carers.

Social networking and personal publishing and other forms of social media communication

- The school will educate the school community in the safe use of social networking sites, and consider how to educate pupils and staff in their safe use.

- Pupils will be advised never to give out personal details of any kind which may identify them, their friends or their location.

- Pupils must be made aware of how they can report abuse and who they should report abuse to.

- Pupils should be taught the reasons why personal photos should not be posted on any social network space without considering how the photo could be used now or in the future.

- Pupils and parents will be advised that the use of social network spaces outside school brings a range of dangers for primary aged pupils.

- Pupils will be advised to use nicknames and avatars when using internet based social networking sites.

- Pupils should be advised on security and encouraged to set passwords, to deny access to unknown individuals and block unwanted communications. Pupils should only invite known friends and deny access to others.

Managing, monitoring and filtering

- The school will work with Wigan LA, and Virtue Technologies to ensure systems to protect pupils are reviewed and improved.

- If staff or pupils come across unsuitable on-line materials, the site must be reported to the Online Safety Officer (Stuart Colothan—Headteacher).

- Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

Managing videoconferencing & webcam use

- Video conferencing should use the Wigan educational network to ensure quality of service and security.

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

- Video conferencing and webcam use will be appropriately supervised for the pupil's age.

Managing emerging technologies

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

- The senior leadership team should note that technologies such as mobile phones and IPads with wireless Internet access can bypass school filtering systems and present a new route to undesirable material and communications. Staff will monitor and supervise all use of Ipads.

- Where contact with pupils is required to facilitate their learning, staff will be issued with a school phone. (See Mobile Phone Policy)

- Mobile phones will not be allowed in school during lessons or formal school time. The sending of abusive or inappropriate text messages or files by Bluetooth or any other means is forbidden. (See Mobile Phone Policy)

- The use of cameras in mobile phones is currently not allowed. (See Mobile Phone Policy)

- Games machines including the Sony PlayStation, Microsoft Xbox and others have Internet access which may not include filtering. Care is required in any use in school or other officially sanctioned location.

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

- All staff, volunteer helpers and students must read and sign to show agreement with the "Acceptable Use Policy for Staff" before using any school Computing resource, including IPads/laptops used for professional use.

- The school will maintain a current record of all staff and pupils who are granted access to school ICT systems.

- At Key Stage 1 and 2, access to the Internet will be by adult demonstration with supervised access. Pupils will be advised to use the preferred search engine 'KidRex' to help them search safely.

- Pupils, parents and carers will be asked to sign and return an "Acceptable Use for pupils" (Computer Rules) consent form. This is generally completed at Parents Evenings or on entry to the school.

Assessing risks

- The school will take all reasonable precautions to prevent access to inappropriate 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 computer connected to the school network. Neither the school nor Wigan can accept liability for any material accessed, or any consequences of Internet access.

- The school will maintain a log of computer usage to enable Impero (monitoring software) violations to be traced. This will be via personal log ons from Year 1 upwards for all staff and pupils.

- Other users of the school server for example students, supply and parents (at training sessions) will be monitored and logged by SLT supported by the Computing subject leaders.

- Staff will be given a copy of the school's guidelines for 'What happens if' scenarios and forms part of the Induction for staff and volunteers.

- The school should audit ICT use to establish if the Online Safety policy is adequate and that the implementation of the Online Safety policy is appropriate and effective. See Appendix 1 for examples of pupil voice questions.

Handling Online Safety complaints

- Staff will adhere to the School Online Safety Guidelines.

- Complaints of Internet misuse will be reported to the Online Safety lead and action in line with the Wigan Safeguarding Children Board Online Safety policy will be taken.

- Any staff misuse that suggests a crime has been committed, a child has been harmed or that a member of staff is unsuitable to work with children should be reported to the LADO (Local Authority Designated Officer) within one working day in accordance with Wigan Safeguarding Board policies.

- Any complaint about staff misuse must be referred to the Headteacher and if the misuse is by the Headteacher it must be referred to the Chair of Governors in line with Wigan Safeguarding Board Child Protection Procedures.

- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.

- Pupils, parents and staff will be informed of the complaints procedure.

Parents and carers attention will be drawn to the School Online Safety Policy in newsletters, the school brochure, on the Online Safety page on the school Website and regular communications specifically on Online Safety. Parents and carers will receive a copy of the Online Safety guidance brochure "Children Computing and Online Safety" and other appropriate literature to discuss with their children including Digital Parenting Magazine.

The school will maintain a list of Online Safety resources for parents/carers.

Opportunities will be given for parents and carers to attend workshops/meetings with resources available to support parents with parental control measures at home. The school website will feature such resources to download.

The school will ask all new parents/carers to sign the "Acceptable Use for pupils" document when they register their child with the school.

Monitoring and Review

The Headteacher monitors the effectiveness of this policy on a regular basis. The Headteacher also reports to the governing body on the effectiveness of the policy and, if necessary, makes recommendations for further improvements.

Signed:

Headteacher: Mr. S. Colothan

Date: June 2017

A Achieve
B Believe
C Care
at St Wilfrid's we can

Appendix 1

Sample questions for pupils

1. If you felt uncomfortable about anything you saw or if anybody asked you for your personal details such as your address on the internet would you know where to go for help?
2. If anybody sent you hurtful messages on the internet or on your mobile phone would you know who to tell?
3. Can you tell me one of the rules your school has for using the internet?
4. Do you understand what the risks of posting inappropriate content on the internet are?

Appendix 2

Click Clever Click Safe

Zip it

Keep your personal stuff private and think about what you say and do online

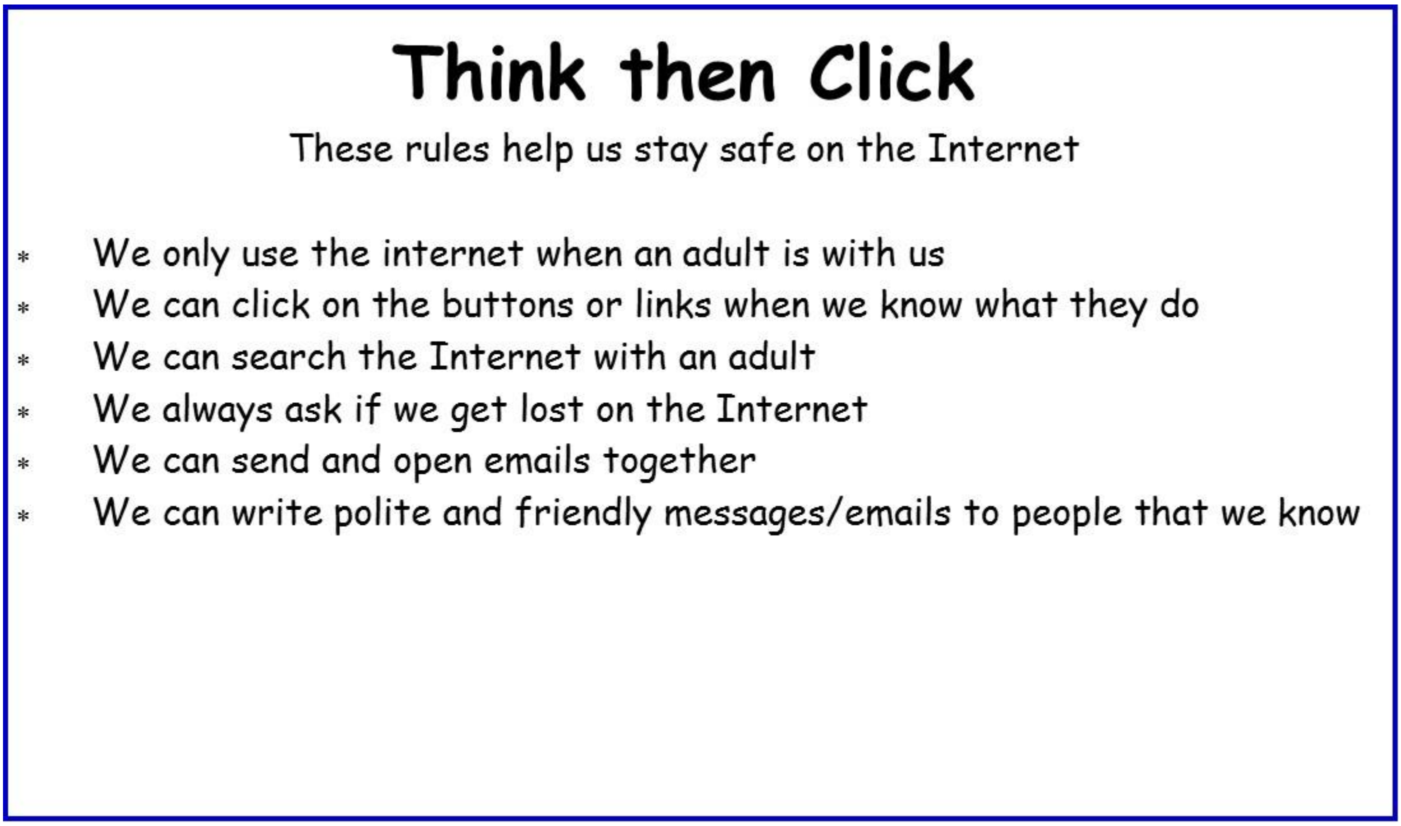
Block it

Block people who send nasty messages and don't open unknown links and attachments

Flag it
Flag up with someone you trust if anything upsets you of if someone asks you to meet offline.

Appendix 3

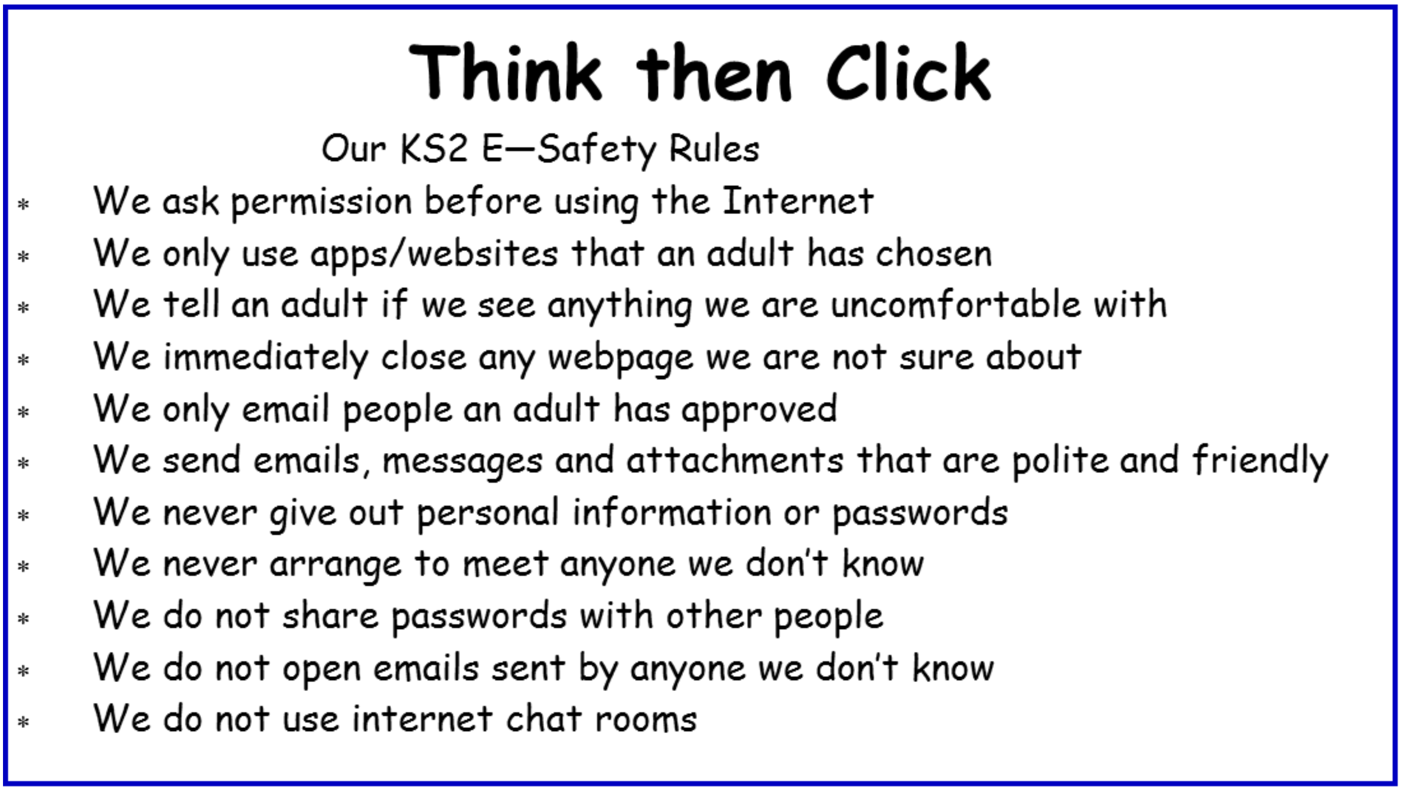
Our rules to help us stay safe online.



Think then Click

These rules help us stay safe on the Internet

- We only use the internet when an adult is with us
- We can click on the buttons or links when we know what they do
- We can search the Internet with an adult
- We always ask if we get lost on the Internet
- We can send and open emails together
- We can write polite and friendly messages/emails to people that we know



Think then Click

Our KS2 E—Safety Rules

- We ask permission before using the Internet
- We only use apps/websites that an adult has chosen
- We tell an adult if we see anything we are uncomfortable with
- We immediately close any webpage we are not sure about
- We only email people an adult has approved
- We send emails, messages and attachments that are polite and friendly
- We never give out personal information or passwords
- We never arrange to meet anyone we don't know
- We do not share passwords with other people
- We do not open emails sent by anyone we don't know
- We do not use internet chat rooms

Appendix 4

Responding to & managing sexting incidents

Context
With the rise of sexting incidents involving young people, this guidance aims to help schools identify sexting incidents, manage them and escalate appropriately.

For school staff
Remember: The production and distribution of sexting images involving anyone under the age of 18 is illegal and needs very careful management for all those involved.

Step 1:
If a device is involved – Confiscate it and set it to flight mode or, if not possible, switch it off

Step 2:
Seek advice – report to your designated safeguarding lead via your normal child protection procedures.

For the designated safeguarding lead

Record all incident of sexting, include both the actions you did take as well as the actions you didn't take and give justifications. In applying judgements to each incident, consider the following:

· Is there a significant age difference between the sender/receiver involved?

· Is there any external coercion involved or encouragement beyond the sender/receiver?

· Do you recognise the child as more vulnerable than usual i.e. at risk?

· Is the image of a severe or extreme nature?

· Is the situation isolated or has the image been more widely distributed?

· Have these children been involved in a sexting incident before?

· Are there other circumstances relating to either sender or recipient that may add cause for concern i.e. Difficult home circumstances?

If any of these circumstances are present, then do escalate or refer the incident using your normal child protection procedures. This includes reporting to the police.

If none of these circumstances are present, then manage the situation accordingly within the school and without escalating to external services. Record the details of the incident, action and resolution.

Appendix 5
Online Safety incident report form

This form should be kept on file by the designated safeguarding lead.

St Wilfrid's Church of England Primary Academy
Rectory Lane
Standish
Wigan
WN6 0XB

Designated Online Safety Officer:

Email: headteacher@admin.saintwilfrids.wigan.sch.uk Tel: 01257 423992

Details of incident:

Time: **Date:**

Name of person reporting incident:

If not reported how was the incident identified?

Where did the incident occur?

□ In school/service setting □ Outside school/service setting

Who was involved in the incident?

□Child/young person □staff member □other (please specify)

Type of incident:

□Bullying or harassment (cyber bullying) □Child abuse images

□Deliberately bypassing security access □On-line gambling

□Hacking or virus propogation □Soft core pornographic material

□Racist, sexist, homophobic, religious hate material □Illegal hard core pornographic material

□Terrorist material □Other (please specify)

□Drug/bomb making material

Description of incident:

Action taken: