HOLY TRINITY
CE PRIMARY SCHOOL

Online safety and Social Media policy

Learning and caring together, building a firm foundation for the future

Date Policy adopted: June 2015

Date to be revisited: June 2017

- Our e-Safety Policy has been written by the school, building on the KCC e-Safety Policy and government guidance.
- Our School Policy has been agreed by the Senior Leadership Team and approved by governors.
- Our School Policy has been approved by the School Council.
- The School has appointed a member of the Governing Body, Deborah Bowler, to take lead responsibility for e-Safety.

The School e-Safety Coordinators are Mr D Turner (Online safety Curriculum Leader) And Mrs K O'Connor (Online safety Safeguarding Leader).

Policy approved by Head Teacher: Mr Beazeley Date: ……

Policy approved by Governing Body: …….. (Chair of Governors)

Date: ……

Policy approved by School Council Date: Wednesday the 10th of June 2015

The date for the next policy review is June 2017

Teaching and learning

Why is Internet use important?

- Internet use is part of the statutory curriculum and is a necessary tool for learning.
- The Internet is a part of everyday 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.
- Pupils use the Internet widely outside school and need to learn how to evaluate Internet information and to take care of their own safety and security.

How can Internet use enhance learning?

- The school's Internet access will be designed to enhance and extend education.
- Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.
- The schools will ensure that the copying and subsequent use of Internet-derived materials by staff and pupils complies with copyright law.
- Pupils will be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

- Pupils will use age-appropriate tools to research Internet content such as 'Aquabrowser', 'KidRex' and 'Google Safe Search kids'.

Managing Information Systems

How will information systems security be maintained?

- The security of the school information systems and users will be reviewed regularly.
- Virus protection will be updated regularly.
- Personal data taken off site will be encrypted.
- Portable media may not used without specific permission followed by an anti-virus / malware scan.
- The use of user logins and passwords to access the school network will be enforced.

How will email be managed?

- Pupils may only use approved email accounts for school purposes.
- Whole -class or group email addresses will be used for communication outside of the school.
- Pupils must immediately tell a designated member of staff if they receive offensive email.
- Pupils must not reveal personal details of themselves or others in email communication, or arrange to meet anyone without specific permission from an adult.
- Staff will only use official school provided KLZ email accounts for all work related e-mails.

How will website content be managed? Can pupils' images or work be published?

- The contact details on the website will be the school address, email and telephone number. Staff or pupils' personal information will not be published.
- 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/videos of pupils are electronically published.

How will social networking, social media be managed?

- Pupils will be advised never to give out personal details of any kind which may identify them and/or their location. Examples would include real name, address, mobile or landline phone numbers, school attended, IM and email addresses, full names of friends/family, specific interests and clubs.
- Pupils will be advised on security and privacy online and will be encouraged to set passwords, deny access to unknown individuals and to block unwanted communications. Pupils will be encouraged to approve and invite known friends only on social networking sites and to deny access to others by making profiles private.
- Concerns regarding students' use of social networking, social media and personal publishing sites (in or out of school) will be raised with their parents/carers.

- Staff personal use of social networking, social media and personal publishing sites will be discussed as part of staff induction and safe and professional behaviour will be outlined in the school Acceptable Use Policy.

How will filtering be managed?

- The school's broadband access will include filtering appropriate to the age and maturity of pupils.
- The school will work with KCC and the Schools Broadband team to ensure that filtering policy is continually reviewed.
- The school will have a clear procedure for reporting breaches of filtering (as per school e-safety concern flowchart). If staff or pupils discover unsuitable sites, the URL will be reported to the School e-Safety Coordinators who will then record the incident and escalate the concern as appropriate.

How will videoconferencing be managed?

- All videoconferencing equipment in the classroom must be switched off when not in use and not set to auto answer.

Users:

- Pupils will ask permission from a teacher before making or answering a videoconference call.
- Videoconferencing will be supervised appropriately for the pupils' age and ability.
- Parents and carers consent should be obtained prior to children taking part in videoconferences.

Content:

- When recording a videoconference lesson, written permission should be given by all sites and participants. The reason for the recording must be given and the recording of videoconference should be clear to all parties at the start of the conference. Recorded material shall be stored securely.
- Videoconferencing is a challenging activity with a wide range of learning benefits. Preparation and evaluation are essential to the whole activity.
- Establish dialogue with other conference participants before taking part in a videoconference. If it is a non school site it is important to check that they are delivering material that is appropriate for your class.

How are emerging technologies and mobile phones managed?

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed. Many emerging communications technologies offer the potential to develop new teaching and learning tools, including mobile communications, Internet access, collaboration and multimedia tools. A risk assessment needs to be undertaken on each new technology for effective and safe practice in classroom use to be developed. The safest approach is to deny access until a risk assessment has been completed and safety has been established.

- Mobile phones will not be used during lessons or formal school time. Mobile phone devices will be held in a secure place in the school office.

- The sending of abusive or inappropriate messages or content via mobile phones or personal devices is forbidden by any member of the school community and any breaches will be dealt with as part of the school discipline/behaviour policy.

How will Internet access be authorised?

- All staff will read and sign the School Acceptable Use Policy before using any school ICT resources.
- All visitors to the school site who require access to the schools network or internet access will be asked to read and sign an Acceptable Use Policy.
- Parents will be informed that pupils will be provided with supervised Internet access appropriate to their age and ability.
- Pupils' access to the Internet will be supervised. Pupils will use age-appropriate search engines and online tools and online activities will be teacher-directed where necessary.

How will risks be assessed?

- The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the global and connected nature of Internet content, it is not possible to guarantee that access to unsuitable material will never occur via a school computer. Neither the school nor KCC can accept liability for the material accessed, or any consequences resulting from Internet use.
- The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990 and breaches will be reported to Kent Police.
- Methods to identify, assess and minimise risks will be reviewed regularly.

How will the school respond to any incidents of concern?

- All members of the school community will be informed about the procedure (as per school e-safety concern flowchart) for reporting e-Safety concerns (such as breaches of filtering, cyberbullying).
- The e-Safety Coordinators will record all reported incidents and actions taken in the School e-Safety incident log and other in any relevant areas e.g. Bullying or Child protection log.
- The Designated Child Protection Coordinator will be informed of any e-Safety incidents involving Child Protection concerns, which will then be escalated appropriately.
- The school will manage e-Safety incidents in accordance with the school discipline/ behaviour policy where appropriate.
- The school will inform parents/carers of any incidents of concerns as and when required.
- Any complaint about staff misuse will be referred to the head teacher.

How will Cyberbullying be managed?

- Cyberbullying (along with all other forms of bullying) of any member of the school community will not be tolerated.
- There are clear procedures (as per school e-safety concern flowchart) in place to support anyone in the school community affected by cyberbullying.
- All incidents of cyberbullying reported to the school will be recorded.
- Pupils, staff and parents/carers will be advised to keep a record of the bullying as evidence.
- Sanctions for those involved in cyberbullying may include:
    - The bully will be asked to remove any material deemed to be inappropriate or a service provider may be contacted to remove content if the bully refuses or is unable to delete content.
    - Internet access may be suspended at school for the user for a period of time. Other sanctions for pupils and staff may also be used in accordance to the schools anti-bullying, behaviour policy.
    - Parent/carers of pupils will be informed.
    - The Police will be contacted if a criminal offence is suspected.

How will parents' support be enlisted?

- Our school e-safety policy will be available from reception and will be added to the e-safety page of our school website.
- A partnership approach to e-Safety at home and at school with parents will be encouraged. Information and guidance for parents on e-Safety will be made available to parents in a variety of formats. This will include offering parental e-safety guidance sessions, advice on our website and via letters home. The digital parenting magazine will also be made available on our website and a hard copy of the magazine sent to parents and carers.
- Parents will be requested to sign an Internet agreement as part of the Home School Agreement.
- Advice on useful resources and websites, filtering systems and educational and leisure activities which include responsible use of the Internet will be made available to parents.